Paavo Terva

Zero Trust -arkkitehtuuri

Opinnäytetyö
Tieto- ja viestintätekniikka

2020

Tekijä/Tekijät	Tutkinto	Aika
Paavo Terva	Insinööri (AMK)	Marraskuu 2019

Opinnäytetyön nimi

Zero Trust -arkkitehtuuri

38 sivua
14 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu

Ohjaaja

Vesa Kankare

Tiivistelmä

Tässä opinnäytetyössä tutustutaan Zero Trust -arkkitehtuuriin, sen toimintaperiaatteeseen ja arkkitehtuurin mahdollistaviin työkaluihin. Opinnäytetyön tutkimusongelmat ovat Zero Trust -arkkitehtuurin yksityiskohtainen selittäminen ja sen implementoiminen virtuaalisessa laboratorioympäristössä. Aiheen teoreettisen käsittelyn lisäksi opinnäytetyö muodostuu käytännön osuudesta, jossa luodaan Zero Trust -arkkitehtuurin periaatteita noudattava verkko soveltuvuusselvityksenä Kaakkois-Suomen ammattikorkeakoulun virtuaaliselle laboratorioympäristölle, eli VirtualLab-alustalle.

Zero Trust -arkkitehtuurin tavoitteena on korjata perinteisten tietoturva-arkkitehtuurien perustavanlaatuisia ongelmia, jotka liittyvät luottamukseen. Arkkitehtuuri pyrkii eliminoimaan käsityksen luottamuksesta kokonaisuudessaan. Arkkitehtuurissa oletetaan, että tietoturvauhkia voi olla ulkoverkon lisäksi myös sisäverkossa. Zero Trust -arkkitehtuurin mukaiset periaatteet on mahdollista saavuttaa moderneilla työkaluilla, kuten verkon mikrosegmentoinnilla, monitasoisella autentikoinnilla, julkisten avainten hallintajärjestelmillä ja uuden sukupolven palomuureilla.

Käytännön osiossa tutkitaan ZeroTier-palvelua ja sen käyttöönottoa VirtualLab-alustalla. Osio muodostuu ZeroTier-palvelun toimintaperiaatteen tutkimisesta ja sen käyttöönottamisesta Zero Trust -arkkitehtuurin tarpeet huomioon ottaen.

Opinnäytetyön lopputuloksena on kattava teoriaosio Zero Trust -arkkitehtuurista ja siihen liittyvistä käsitteistä. Käytännön osiossa tutkitaan ZeroTier-palvelua, ja osioon sisältyy ohje palvelun implementoinnista VirtualLab-alustalle.

Asiasanat

Zero Trust, ZeroTier, tietoturva, tietoturva-arkkitehtuuri, autentikointi, auktorisointi

Author (authors)	Degree	Time
Paavo Terva	Bachelor of Engineering	November 2019

Thesis title

Zero Trust Architecture

38 pages
14 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences (Xamk)

Supervisor

Vesa Kankare

Abstract

In this thesis, the objective was to explore Zero Trust Architecture, its operational principles and the tools that make the architecture possible. The research problems were explaining Zero Trust Architecture in detail and implementing the architecture in a virtual laboratory environment. In addition to theoretical explanation, the thesis includes an experimental study, where a Zero Trust Architecture network was implemented as a proof-of-concept in South-Eastern Finland University of Applied Sciences' virtual laboratory environment, VirtualLab.

The objective of Zero Trust Architecture is to fix the fundamental problems of traditional security architectures concerning trust. The architecture aims to eliminate the concept of trust in its entirety and assumes that security threats are present both outside and inside of a network. The principles of Zero Trust Architecture are achievable with modern tools, such as network microsegmentation, Multi-Factor Authentication, Public Key Infrastructure and Next-Generation Firewalls.

In the experimental study, the product ZeroTier was examined and implemented in VirtualLab. The study consists of two parts: explaining the product's operational principles and implementing the product based on the requirements of Zero Trust Architecture.

The result of this thesis is a comprehensive theoretical explanation of Zero Trust Architecture and the concepts related to it. In the experimental study, the product ZeroTier was explored. Also, this thesis provides instructions on how to implement ZeroTier in Xamk's VirtualLab.

Keywords

Zero Trust, ZeroTier, security, security architecture, authentication, authorization

SISÄLLYS

1 JOHDANTO

Maailman väkiluku kasvaa nopeasti, mutta Internetin käyttäjien määrä kasvaa vielä nopeammin. Vuonna 2019 maailman yli 7,7 miljardista ihmisestä yli 4,5 miljardilla oli pääsy Internetiin. Vuonna 2009 tämä luku oli vain 1,8 miljardia, mikä tarkoittaa kymmenien, jopa satojen miljoonien vuosittaista nousua käyttäjien määrässä. Kasvu on eksponentiaalista, eikä se ole näyttämässä merkkejä heikkenemisestä. (Internet World Stats 2019.)

Jatkuvan digitalisaation johdosta näiden miljardien ihmisten henkilötietoja on useiden yritysten tietokannoissa. Henkilötiedoista on tullut arvokas tuote, joten ei ole ihme, että myös tietomurrot ovat kasvaneet sekä määrältään että laajuudeltaan. Vuoden 2019 kesäkuun loppuun mennessä yritykset olivat menettäneet yli 4,1 miljardia tallennetta tietomurtojen seurauksena. Todellinen luku on todennäköisesti paljon suurempi, koska moni tietomurroista jää huomaamatta, eikä kaikista tietomurroista tiedoteta julkisesti. (Risk Based Security 2019.)

Varoittavana esimerkkinä tietomurtojen taloudellisista vaikutuksista on muun muassa Yahoo!-yhtiön kokemat tietomurrot vuosina 2013–2016. Kyseessä oli yksi maailman suurimmista tietomurroista, joka koski kolmea miljardia palvelussa olevaa käyttäjätiliä. Tämä johti siihen, että yhtiön arvo laski sadoilla miljoonilla dollareilla, minkä lisäksi yhtiö on joutunut maksamaan kymmeniä miljoonia sakkoja ja korvauksia asianomaisille. (Reuters 2019.)

Tietoturvaratkaisuja tarjoavat yritykset kehittävät jatkuvasti uusia keinoja jatkuvasti kasvavien tietomurtojen estämiseksi. Yksi näistä keinoista on Zero Trust -arkkitehtuuri, jonka toimintaperiaatetta ja käyttöönottoa käsitellään tässä opinnäytetyössä. Nimensä mukaisesti Zero Trust -arkkitehtuurin tavoitteena on estää tietomurtojen tapahtuminen poistamalla käsite luottamuksesta organisaation verkkoarkkitehtuurin osalta. Arkkitehtuuri perustuukin englanninkieliseen periaatteeseen: ”never trust, always verify”. (Palo Alto Networks s.a.)

1.1 Opinnäytetyön tavoite

Tämän opinnäytetyön tavoitteena on selittää Zero Trust -arkkitehtuurin toimintaperiaatetta ja luoda arkkitehtuurin perustuva verkko virtualisoituun laboratorioympäristöön, joka on tässä tapauksessa Kaakkois-Suomen ammattikorkeakoulun oma VirtualLab-pilvipalvelualusta. Tämän opinnäytetyön kirjoitushetkellä Zero Trust -arkkitehtuuri on uudehko konsepti, mistä syystä tutkimusongelmiksi muodostuvat arkkitehtuurin selittäminen teoriassa ja sen implementoiminen käytännössä. Opinnäytetyössä pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Mitä Zero Trust -arkkitehtuuri on?
- Miten Zero Trust -arkkitehtuurin toimintaperiaate vertautuu perinteisiin tietoturva-arkkitehtuureihin?
- Miten Zero Trust -arkkitehtuuri voidaan implementoida virtualisoidussa laboratorioympäristössä (VirtualLab-alusta)?

Opinnäytetyö jakautuu näiden kysymysten perusteella kahteen osaan: teoreettiseen ja käytännölliseen osaan. Teoreettisen osan tavoitteena on selittää Zero Trust -arkkitehtuurin toimintaperiaate. Toimintaperiaatteen määrittelyn lisäksi opinnäytetyössä pohditaan arkkitehtuurin hyviä ja huonoja puolia sekä verrataan sitä perinteisiin tietoturva-arkkitehtuureihin erilaisista näkökulmista, kuitenkin tietoteknistä näkökulmaa painottaen.

Käytännöllisen osan tavoitteena on implementoida Zero Trust -arkkitehtuuriin perustuva verkko VirtualLab-alustalle. Jos verkon implementointi onnistuu, opinnäytetyöhön sisällytetään ohje, jossa käydään kyseisen verkon rakentamisprosessi läpi askel askeleelta. Kaakkois-Suomen ammattikorkeakoulu voi käyttää tätä ohjetta tulevaisuudessa, jos koulutusohjelman kursseihin sisältyy jatkossa Zero Trust -arkkitehtuuri. Ohje voi myös toimia lähteenä tuleville opinnäytetöille, mikäli arkkitehtuurin implementointia virtuaalisessa laboratorioympäristössä halutaan kehittää eteenpäin.

Zero Trust -arkkitehtuuri ja sen implementoiminen virtualisoituun laboratorioympäristöön on aihe, jota ei ole käsitelty aikaisemmissa opinnäytetöissä. Tästä syystä opinnäytetyö ei perustu mihinkään olemassa olevaan ratkaisuun, vaan arkkitehtuurin tutkiminen sekä teoriassa että käytännössä aloitetaan

”puhtaalta pöydältä”. Muita opinnäytetöitä, joissa VirtualLab-alustalle on implementoitu tietty ominaisuus ovat esimerkiksi MPLS Segment Routing Technology Study (Varkama 2017) ja Implementing a Private Cloud with System Center 2016 in a Virtual Lab Environment (Svobunas 2017). Tämän opinnäytetyön käytännöllisessä osassa voidaan käyttää hyväksi näissä opinnäytetöissä havaittuja ratkaisuja VirtualLab-alustaa koskevissa ongelmatilanteissa.

1.2 Opinnäytetyön tutkimusmenetelmä

Tämän opinnäytetyön tutkimusmenetelmäksi on valittu kehittämistutkimus. Kehittämistutkimuksen tarkoituksena on tuottaa toimivia käytännön ratkaisuja, mutta kehitettävän kohteen lisäksi kehittämistutkimuksessa on oltava myös tutkimuksellinen ote. Kehittämistutkimuksessa voidaan käyttää tutkimuksen luonteesta riippuen sekä kvalitatiivisia että kvantitatiivisia tutkimusmenetelmiä. (Kananen 2012, luku 2.)

Näiden ominaisuuksien ansiosta kehittämistutkimus sopii tämän opinnäytetyön tutkimusmenetelmäksi parhaiten. Zero Trust -arkkitehtuurin toimintaperiaatteen selittäminen tuo tarvittavaa tutkimuksellisuutta opinnäytetyöhön. Tässä opinnäytetyössä tutkimusmenetelmät ovat pitkälti kvalitatiivisia eli laadullisia, koska tavoitteena on ymmärtää opinnäytetyössä käsiteltävää konseptia.

Opinnäytetyöstä saatava lopputulos on tietoa Zero Trust -arkkitehtuurista ja VirtualLab-alustasta. Jos arkkitehtuurin implementoiminen onnistuu, sitä voidaan hyödyntää jatkossa esimerkiksi opetustarkoituksessa. Uuden arkkitehtuurin käyttäminen virtualisoidussa laboratorioympäristössä tuo uusia mahdollisuuksia myös tuleviin opinnäytetöihin. Jos toimeksiantona on esimerkiksi Zero Trust -arkkitehtuuriin perustuvan verkon rakentaminen tietylle yritykselle, niin tehtävää on huomattavasti helpompi lähestyä, jos arkkitehtuurin simulointi VirtualLab-alustalla on todistettu toimivaksi.

2 ZERO TRUST -ARKKITEHTUURI

2.1 Käsitteen synty

Käsitteenä Zero Trust -arkkitehtuuri on suhteellisen uusi. Se sai alkunsa vuonna 2010, kun Forrester Research -yrityksen silloinen analyytikko John Kindervag totesi perinteisten tietoturvamallien perustuvan vanhentuneeseen periaatteeseen, jossa organisaation sisäverkossa oleviin käyttäjiin ja laitteisiin luotetaan sokeasti. Nämä tietoturvamallit olettavat, että kriittisillä käyttöoikeuksilla varustetut tunnukset eivät joudu vääriin käsiin. (Palo Alto Networks s.a.)

Zero Trust -arkkitehtuuri pyrkii ratkaisemaan tämän luottamuksesta aiheutuvan ongelman poistamalla käsitteen luottamuksesta kokonaisuudessaan organisaation verkkoarkkitehtuurissa. Perinteisten tietoturva-arkkitehtuurien periaatteena voisi pitää sanontaa: ”trust, but verify”. Zero Trust -arkkitehtuurissa luottamus on eliminoitu sanontaa myöten: ”never trust, always verify”. (Mt.)

2.2 Zero Trust eXtended ecosystem

Arkkitehtuurin alun perin kehittänyt yritys Forrester Research julkaisee vuosittain Zero Trust eXtended ecosystem -raportin, joka sisältää tietoa merkittävien Zero Trust -ratkaisujen toimittajista ja pisteyttää yritysten kehittämiä ratkaisuja erilaisilla kriteereillä. Raporttiin sisällytettyjä yrityksiä voidaan pitää arkkitehtuurin pioneereina. Vuoden 2019 raporttiin sisällytettiin seuraavat yritykset:

- Akamai Technologies
- Check Point
- Cisco
- Cyxtera Technologies
- Forcepoint
- Forescout
- Google
- Illumio
- MobileIron
- Okta
- Palo Alto Networks
- Proofpoint
- Symantec
- Unisys (Cunningham 2019.)

2.3 Nykytilanne ja tulevaisuus

Edellä listattujen yritysten lisäksi Zero Trust -ratkaisuja tarjoavat muutkin listan ulkopuolelle jäävät organisaatiot, ja erilaisten ratkaisujen määrän odotetaan nousevan jatkuvasti arkkitehtuurin suosion ja tietoturvan merkityksen kasvaessa. Syynä arkkitehtuurin suosion nopeaan kasvuun on muun muassa se, että suuret organisaatiot ovat implementoineet Zero Trust -ratkaisuja hyvällä menestyksellä. Suurista yrityksistä esimerkiksi Google on kehittänyt yhden tunnetuimmista ratkaisuista BeyondCorp-viitekehyksellään. (Google s.a.).

Yritysten panostaessa enemmän tietoturvansa parantamiseen, erilaiset Zero Trust -ratkaisut voivat vaikuttaa parhaimmilta vaihtoehdoilta perinteisiin tietoturva-arkkitehtuureihin verrattuna, koska arkkitehtuuri on saanut ylistystä tunnetuilta tahoilta ja sen premissinä on vanhentuneiden ratkaisujen puutteiden korjaaminen. Arkkitehtuurin markkina-arvon on tutkittu nousevan nykyisestä 15,6 miljardista dollarista 38,6 miljardiin dollariin vuoteen 2024 mennessä (Markets and Markets 2019).

3 AIHEESEEN LIITTYVIÄ KÄSITTEITÄ

3.1 OSI-malli

Open Systems Interconnection eli OSI-malli on universaali viitekehys, jonka tarkoituksena on jakaa tietoliikenne erilaisiin käsitteellisiin kerroksiin ja selittää tietoliikenteen toimintaperiaatetta niiden avulla. OSI-mallissa on seitsemän kerrosta. Kerrosten ja niiden välisen vuorovaikutuksen ymmärtäminen on hyvä tapa analysoida myös Zero Trust -arkkitehtuuriin perustuvia verkkoja. Mallin kerrokset ovat alhaalta ylöspäin seuraavat:

1. Fyysinen kerros
2. Siirtokerros
3. Verkkokerros
4. Kuljetuskerros
5. Istuntokerros
6. Esitystapakerros
7. Sovelluskerros (ISO/IEC 7498-1: 1994)

Fyysinen kerros sisältää kaikki tietoliikenteen vastaanottamiseen ja lähettämiseen käytettävät fyysiset osat, kuten reitittimet ja kytkimet, niiden väliset liitännät ja kaapeloinnin. Verkon välityksellä lähetettävä data muutetaan biteiksi fyysisessä kerroksessa, ja bittejä voidaan lähettää esimerkiksi radiosignaalien, sähköimpulssien tai valon muodossa. (Mt.)

Siirtokerroksen tehtävänä on huolehtia sisäverkon yhteyksien luomisesta ja purkamisesta. Siirtokerroksessa varmistetaan, että lähetettävä data siirretään oikealla nopeudella, jotta datan vastaanottaja kykenee käsittelemään sitä. Fyysisessä kerroksessa saattaa ilmetä virheitä, ja näiden virheiden korjaus on tarkoitus suorittaa siirtokerroksessa. (Mt.)

Verkkokerroksessa data liikennöidään sisäverkon ulkopuolelle optimaalisia fyysisiä reittejä käyttäen. Tämä reitittämisenä tunnettu prosessi ei ota huomioon sisäverkon fyysistä rakennetta. Reitittäminen tapahtuu erilaisten reititysprotokollia ja laitteiden IP-osoitteita käyttämällä. (Mt.)

Kuljetuskerros on vastuussa päätelaitteiden välisestä datan lähettämisestä. Lähettävän osapuolen kuljetuskerroksessa data segmentoidaan pienempiin osiin, jotka kootaan vastaanottavan osapuolen kuljetuskerroksessa ylemmille kerroksille sopivaan muotoon. (Mt.)

Istuntokerroksessa luodaan, ylläpidetään ja puretaan päätelaitteiden välisiä yhteyksiä. Istuntokerroksessa muodostetut istunnot säilyvät aktiivisina niin kauan kuin dataa lähetetään. Jos verkkoyhteys katkeaa odottamattomasti, niin istuntokerroksessa tapahtuvalla datan synkronoinnilla lähetystä voi jatkaa yhteyden palauduttua samasta pisteestä alusta aloittamisen sijaan. (Mt.)

Esitystapakerroksessa varmistetaan, että seuraavan kerroksen, eli sovelluskerroksen sovellukset vastaanottavat datan kyseisille sovelluksille sopivassa muodossa. Datan pakkaaminen, salaaminen ja salauksen purkaminen tapahtuu esitystapakerroksessa. (Mt.)

Sovelluskerros on OSI-mallin ylin kerros. Päätelaitteen käyttäjä hyödyntää esimerkiksi verkkoselainta datan käsittelemistä varten. Tämä verkkoselain puolestaan hyödyntää sovelluskerroksessa olevia rajapintoja ja protokollia, jotta data voidaan esittää käyttäjälle sopivassa muodossa. (Mt.)

3.2 Zero Trust -arkkitehtuuri OSI-mallissa

Jokaisella OSI-mallin kerroksella on oma roolinsa organisaation verkossa ja sen tietoturvallisuudessa. Eri kerroksiin kohdistettavat hyökkäykset ovat erilaisia luonteeltaan, ja myös puolustusmenetelmät ovat erilaisia. Fyysinen kerros voi joutua fyysisten hyökkäysten uhriksi, esimerkkinä murtautuminen verkon toiminnan kannalta kriittisiä laitteita sisältävään kaappiin. Muihin kerroksiin kohdistettavat hyökkäykset ovat luonteeltaan hienovaraisempia, eivätkä ne ole riippuvaisia tietomurron suorittajan maantieteellisestä sijainnista. Esimerkiksi hajautettu palvelunestohyökkäys eli DDoS-hyökkäys on mahdollista toteuttaa OSI-mallin kerroksissa 3, 4, 6 ja 7. (Arbor Networks 2017.)

Zero Trust -arkkitehtuurissa hyödynnettävät teknologiat keskittyvät OSI-mallin 7. kerroksen, eli sovelluskerroksen toimintaperiaatteiden muuttamiseen. Arkkitehtuurille ominaiset ratkaisut, kuten verkon mikrosegmentointi ja politiikkojen sekä sääntöjen hienojakoisuus on mahdollista saavuttaa vain, jos arkkitehtuurin implementointi suoritetaan sovelluskerroksessa. Monet tietomurroista ovat saaneet alkunsa sovelluskerroksen tietoturvan puutteellisuuden takia, joten on loogista, että Zero Trust -arkkitehtuuri pyrkii kehittämään kyseisen kerroksen puolustusmenetelmiä. (Palo Alto Networks s.a.)

3.3 CIA-analysointimalli

Tietoturvaa voidaan analysoida CIA-analysointimallilla. Mallin nimi tulee sanoista confidentiality eli luottamuksellisuus, integrity eli eheys ja availability eli saatavuus. Tietoturvallisessa ympäristössä pyritään saavuttamaan tasapaino näiden kolmen periaatteen välillä. Tasapainon saavuttaminen on tärkeää, koska yhtäkään edellä mainituista periaatteista ei voi noudattaa täydellisesti ilman, että toiset periaatteet kärsisivät. Esimerkiksi liiallinen tiedon saatavuus aiheuttaa haasteita tiedon luottamuksellisuudelle. Tietomurron tapahtuessa yhtä tai useampaa näistä periaatteista on rikottu. (Walkowski 2019.)

Luottamuksellisuudella tarkoitetaan sitä, että suojattavaa tietoa pääsevät käsittelemään ainoastaan henkilöt, joilla on siihen oikeus. Mitä useammalla henkilöllä on oikeus käsitellä tietoa, sitä enemmän mahdollisuuksia hyökkääjällä on tietomurron tekemiseksi. Tämän takia tietoturvallisessa ympäristössä on tärkeää rajoittaa käyttäjien oikeuksia tietojen käsittelyyn. Oikeuksien hallinnalla pienennetään hyökkäyspinnan kokoa ja siten myös mahdollisuudet tietomurtojen tekemiseksi vähenevät. (Mt.)

Eheydellä tarkoitetaan tiedon oikeellisuutta. Tieto voi muuttua sen säilytyksen, käytön ja siirron aikana, ja eheydellä pyritään varmistamaan se, että tietoa ei ole muokattu missään vaiheessa luvattomasti tai vahingossa. Esimerkiksi tiedostonsiirron yhteydessä vastaanottajan tulee saada tiedosto juuri sellaisena kuin se on alun perin lähetetty. (Mt.)

Saatavuudella tarkoitetaan luotettavaa pääsyä tietoihin. Jos henkilön oikeudet suojattuun tietoon ovat kunnossa, hänen tulisi päästä käsittelemään tietoa tarpeen vaatiessa. Tietomurtojen yhteydessä varastetaan rahanarvoista tietoa, mutta joskus tavoitteena voi olla ainoastaan vahingon aiheuttaminen organisaatiolle. Mikäli yrityksen työntekijöillä ei ole pääsyä tietoihin hyökkäyksen takia, siitä voi aiheutua merkittävää taloudellista haittaa esimerkiksi operatiivisen toiminnan keskeytyessä. Toisaalta hyökkäyksen jälkeisissä korjaavissa toimenpiteissä hyökkäyspinta voi mahdollisesti suurentua antaen hyökkääjälle enemmän mahdollisuuksia varsinaisen tietomurron tekemiseksi. (Mt.)

Kaikki organisaatiot eivät pyri identtiseen tasapainoon edellä mainittujen ominaisuuksien osalta, vaan tiettyjä periaatteita korostetaan enemmän suojattavan tiedon luonteesta riippuen. Esimerkiksi valtion tiedustelupalvelut voivat korostaa luotettavuutta, koska suojattava tieto voi olla hyvin arkaluonteista. Pankkien verkoissa puolestaan varmistetaan, että tiedon eheys on korkealla tasolla, koska rahaliikenteessä pienilläkin häiriöillä voi olla suuria taloudellisia seurauksia. (Mt.)

3.4 Zero Trust -arkkitehtuuri ja CIA

CIA-analysointimallin kolmesta periaatteesta Zero Trust -arkkitehtuuri keskittyy eniten luottamuksellisuuteen. Arkkitehtuuriin perustuvassa verkossa käytettävät työkalut lisäävät organisaation verkossa tapahtuvaa autentikointia niin määrällisesti kuin laadullisestikin. Kattavalla autentikoinnilla voidaan saavuttaa huomattavasti luottamuksellisempi verkko muihin tietoturva-arkkitehtuureihin verrattuna, koska käyttäjän oikeellisuutta tarkastellaan kehittyneillä työkaluilla ja aktiivisesti.

Zero Trust -arkkitehtuurin käyttöönotossa ongelmaksi voi muodostua saatavuuden heikkeneminen. Jotta arkkitehtuuri voidaan implementoida onnistuneesti, niin organisaation verkon käyttöoikeudet on dokumentoitava erittäin tarkasti. Jos organisaatiossa ei ole tarkkaa tietoa siitä, mitkä käyttöoikeudet kuuluvat millekin käyttäjälle, niin lopputuloksena on käyttäjän näkökulmasta vaikeapääsyinen verkko. Tällöin saatavuus on heikentynyt. Kuva 1 visualisoi CIA-analysointimallia.

Kuva 1. CIA-analysointimallin kolme periaatetta (Walkowski 2019)

4 ZERO TRUST -ARKKITEHTUURIN TOIMINTAPERIAATE

Zero Trust -arkkitehtuuriin perustuvat ratkaisut voivat olla erilaisia ratkaisun toimittajasta ja organisaation verkon monimutkaisuudesta riippuen. Jokaisen niistä tulisi kuitenkin noudattaa tiettyjä arkkitehtuurille määriteltyjä periaatteita, jotta ne voidaan luokitella aidoiksi Zero Trust -ratkaisuiksi. Tyypillisessä arkkitehtuuriin perustuvassa verkossa otetaan huomioon seuraavat periaatteet kaikissa tietoturvaan liittyvissä asioissa:

- verkko on aina vaarassa
- uhkia on sekä sisä- että ulkoverkossa
- palvelun sijainti verkossa ei vaikuta luottamukseen millään tavalla
- kaikki laitteet, käyttäjät ja liikenne tulee autentikoida ja auktorisoida
- politiikkojen tulee olla dynaamisia ja niiden täytyy perustua useista eri lähteistä tulevaan dataan. (Gilman & Barth 2019.)

Ratkaisut hyödyntävät erilaisia tietoturvateknologioita, kuten monivaiheinen tunnistautuminen, identiteetin hallinta, analytiikka, salaus, pisteyttäminen ja tiedostojärjestelmien käyttöoikeuksien hallinta. Lisäksi käytössä olevia teknologioita tulisi orkestroida eli automatisoida ja sovittaa yhteen, jotta arkkitehtuuria käyttävä verkko olisi helpommin ylläpidettävissä ja käyttökelpoinen myös käyttäjien näkökulmasta. Nämä teknologiat eivät ole Zero Trust -arkkitehtuurille eksklusiivisia, mutta ne implementoidaan osaksi organisaation verkkoa arkkitehtuurin periaatteiden mukaisesti, eli ilman luottamusta mitään tahoa kohtaan. (Secret Double Octopus 2019.)

4.1 Erot perinteisiin arkkitehtuureihin

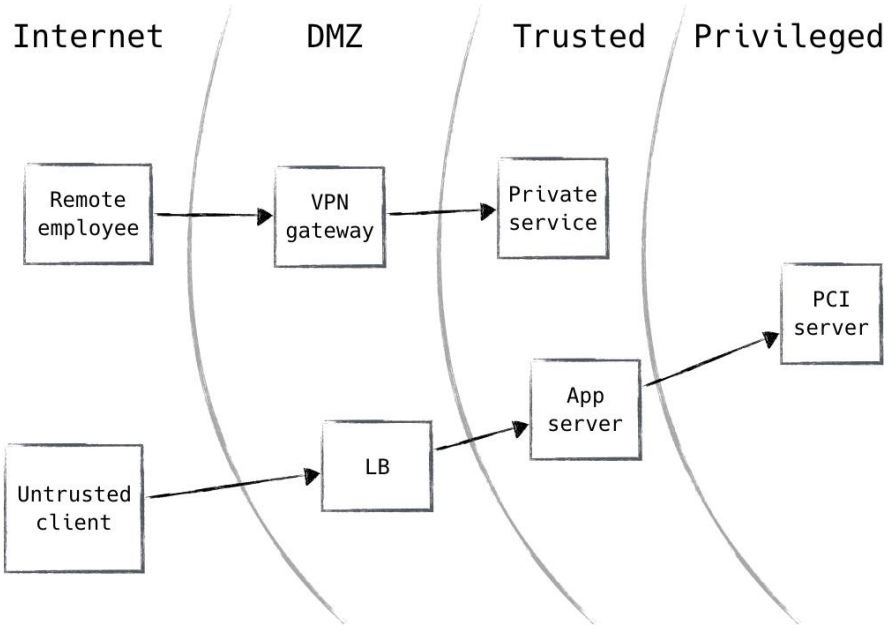
Tietoturva-arkkitehtuurilla tarkoitetaan kokonaisuutta, joka käsittää kaikki verkossa käytettävät tietoturvaratkaisut, oli kyseessä sitten verkon topologia eli rakenne tai käytössä olevat tietoturvatyökalut. Ratkaisut ja käytettävät työkalut määräytyvät organisaation tarpeiden ja vaatimusten mukaan, jotka ovat erilaisia yrityksen koosta ja luonteesta riippuen. Vaikka arkkitehtuureja on mahdollista räätälöidä yrityskohtaisesti, ne noudattavat useimmiten jonkinlaisia periaatteita. Zero Trust -arkkitehtuurin periaatteet poikkeavat perinteisistä tietoturva-arkkitehtuureista monella tapaa. (Gilman & Barth 2017.)

4.1.1 Topologia

Eroavaisuudet näkyvät jo verkon topologiassa. Perinteisen tietoturva-arkkitehtuurin topologia voidaan jakaa alueisiin, jotka palvelevat eri käyttötarkoituksia. Internetin ja organisaation sisäverkon välissä on useimmiten palomuuri, jonka tarkoituksena on suojata sisäverkkoa havaitsemalla Internetistä tulevaa haitallista liikennettä ja estää sen pääseminen sisäverkkoon.

DMZ eli demilitarisoitu alue on perinteisen tietoturva-arkkitehtuurin turvattomin alue, johon sijoitetaan esimerkiksi organisaation sähköpostipalvelimet, julkisen verkon palvelimet ja DNS eli nimipalvelujärjestelmä. Näitä palveluja käyttävät myös organisaation sisäverkon ulkopuolella olevat käyttäjät, ja niihin kohdistuu sisäverkon palveluihin verrattuna enemmän hyökkäyksiä, koska palvelut ulottuvat myös julkiseen verkkoon ja ovat näin ollen helpommin havaittavissa. DMZ-alueen laitteet eivät keskustele suoranaisesti sisäverkon laitteiden kanssa, ja parhaan käytännön mukaisesti ne tulisi eristää sisäverkosta esimerkiksi toisella palomuurilla ja erillisellä aliverkotuksella. (Barracuda s.a.)

Vaikka perinteistä tietoturva-arkkitehtuuria noudattamalla saavutetaan suhteellisen turvallinen verkkoympäristö, se ei ole täysin aukoton. Tietomurroissa käytettävät menetelmät kehittyvät koko ajan, ja perinteisen tietoturva-arkkitehtuurin perustavanlaatuiset puutteet käyvät yhä selkeämmiksi. Näitä puutteita ovat muun muassa sisäverkon liikenteen tutkimisen puute, joustamattomuus sekä fyysisissä että loogisissa sijoituksissa ja yksittäiset pisteet, jotka vikaantuessaan saattavat aiheuttaa häiriöitä koko verkolle. (Gilman & Barth 2019.)



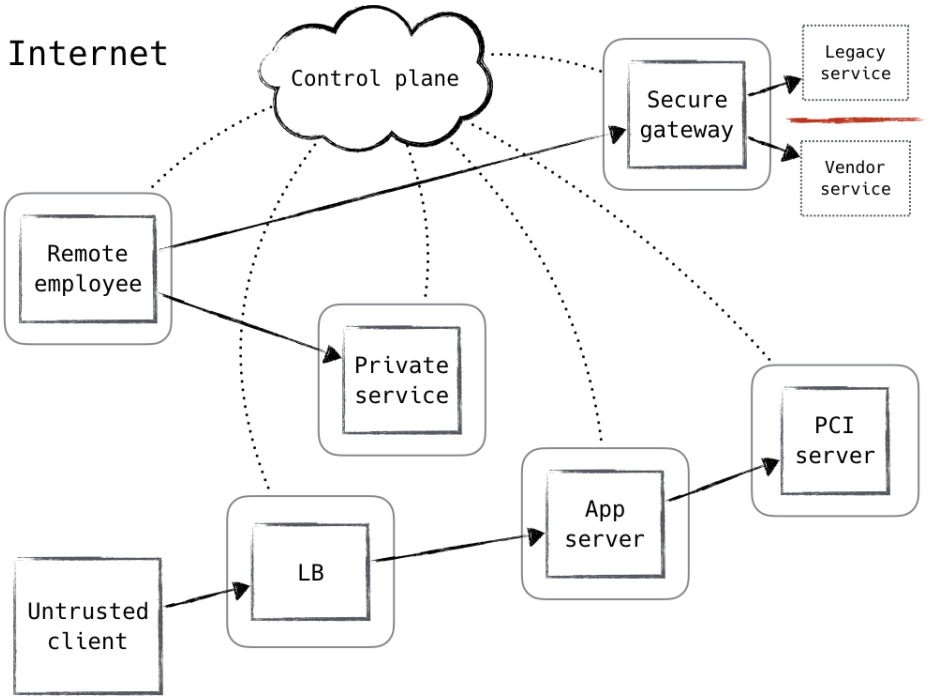
Kuva 2. Perinteinen tietoturva-arkkitehtuuri (Gilman & Barth 2017)

Zero Trust -arkkitehtuuri pyrkii korjaamaan nämä perustavanlaatuiset ongelmat muuttamalla organisaation verkon topologian rakennetta erilaiseksi. Tämä tarkoittaa sitä, että Zero Trust -ratkaisut eivät ole pelkästään olemassa olevien verkkojen päälle asennettavia työkaluja, vaan kyseessä on koko verkon rakenteen uudelleenorganisointi, joka alkaa topologian muuttamisesta Zero Trust -tietoturvatyökaluja parhaiten hyödyntäväksi kokonaisuudeksi. (Mt.)

Tietoturvatyökalut, joita Zero Trust -arkkitehtuuriin perustuvassa verkossa käytetään, hyödyntävät tämän ohjeistuksen perusteella rakennettua topologiaa, ja ohjeistusta voidaan soveltaa myös olemassa oleviin verkkoihin, joskin rakenteelliset muutokset voivat vaikuttaa verkon infrastruktuuriin muutoksen kohteena olevan verkon lähtökohdista riippuen.

Zero Trust -arkkitehtuurin käyttöönotossa voidaan muokata joitakin olemassa olevia ominaisuuksia arkkitehtuurin periaatteiden mukaisiksi. Yksi olennaisimmista ominaisuuksista on hallintapinta eli Control Plane, jonka toimintaperiaatetta muutetaan siten, että autentikointia voidaan vaatia käytännössä jokaisen toimenpiteen kohdalla sen sijaan, että käyttäjälle annettaisiin oikeudet pelkästään palveluun kirjautumisen perusteella. Osa perinteisille tietoturva-arkkitehtuureille tyypillisistä ominaisuuksista on poistettu kokonaan, koska ne ovat joko tarpeettomia Zero Trust -arkkitehtuuria käyttävissä verkoissa, tai niiden käyttötarkoitusta ei voi muokata kyseiselle arkkitehtuurille sopivaksi.

Yksi poistetuista ominaisuuksista on VPN-palvelu, jolle ei ole tarvetta Zero Trust -arkkitehtuuriin perustuvassa verkossa. Palvelun tarkoituksena on luoda suojattu tunneli julkisen ja yksityisen verkon välillä, ja teknologiaa voidaan hyödyntää esimerkiksi etätyöskentelyssä, jolloin tunneli muodostetaan työntekijän kodin verkosta työpaikan sisäverkkoon. Zero Trust -arkkitehtuuriin perustuvassa verkossa liikenne on jatkuvan autentikoinnin alaisena, minkä johdosta tunnelointi on tarpeetonta. VPN-palvelujen välttämättömyyden poistaminen pienentää hyökkäyspintaa, koska myös turvallisina pidetyistä VPN-palveluista on löytynyt haavoittuvuuksia, joita hakkerit voivat hyödyntää tietomurtojen mahdollistamiseksi. (Orange Tsai 2019.)



Kuva 3. Zero Trust -arkkitehtuuri (Gilman & Barth 2017)

Tämä ei tarkoita sitä, että Zero Trust -arkkitehtuurin implementoiminen vaatisi kaikkien vanhojen laitteiden ja palvelujen korvaamista uusilla. Arkkitehtuuriin perustuvia tietoturvaratkaisuja tarjoavan Palo Alto Networksin mukaan Zero Trust -arkkitehtuuriin perustuva verkko on mahdollista rakentaa alusta asti tai olemassa olevan verkon päälle viiden askeleen ohjeistusta noudattamalla. Ohjeistuksen osat ovat:

- suojauspinnan identifioiminen
- verkkoliikenteen kartoittaminen
- Zero Trust -arkkitehtuurin rakentaminen

- Zero Trust -politiikkojen luominen
- monitorointi ja ylläpito. (Palo Alto Networks s.a.)

Suojauspinnalla tarkoitetaan suojattavaa aluetta, joka sisältää organisaation verkon tärkeimpiä tietoja, sovelluksia, laitteita ja palveluja, jotka vaativat tietoturvallisen käyttö- ja säilytysympäristön. Tiedot voivat olla esimerkiksi henkilötietoja, sovellukset organisaation toiminnan kannalta kriittisiä ohjelmistoja, laitteet maksupäätteitä ja palvelut DNS- ja DHCP-palveluja. Näiden suojattavien asioiden määrittelyn jälkeen verkko voidaan mikrosegmentoida, joka tarkoittaa tavallista verkon segmentointia hienojakoisempaa osiin jakamista. (Mt.)

Verkkoliikenteen kartoittamisella pyritään dokumentoimaan, miten organisaation verkossa olevat osat keskustelevat keskenään. Yksi tärkeimmistä asioista Zero Trust -arkkitehtuuriin perustuvan verkon suunnittelussa on vain tarpeellisten oikeuksien jakaminen, ja niiden oikeaoppinen määrittely on helpompaa, kun organisaation verkon liikenteen toiminta on tiedossa. (Mt.)

Vaikka Zero Trust -arkkitehtuuriin perustuvat verkot noudattavat tiettyjä periaatteita, ei ole olemassa mitään yleispätevää mallia, jonka mukaan jokainen verkko voitaisiin rakentaa. Arkkitehtuuria muokataan organisaation tarpeiden mukaisiksi ja arkkitehtuurin mukainen verkko voidaan toteuttaa erilaisilla työkaluilla, esimerkiksi uuden sukupolven palomuureilla. (Mt.)

Arkkitehtuurin implementoimiseen kuuluu Zero Trust -politiikkojen luominen. Politiikat eli erilaiset säännöt ovat yleinen käsite muissakin tietoturva-arkkitehtuureissa, ja Zero Trust -politiikat voidaan määritellä niin kutsutulla Kiplingin metodilla, jossa etsitään vastausta kuuteen kysymykseen:

- Kenellä on pääsy resurssiin?
- Mitä sovellusta käytetään resurssiin pääsyä varten suojauspinnassa?
- Milloin resurssia ollaan käyttämässä?
- Mihin lähetetty paketti on matkalla?
- Miksi tämä paketti on kohdistettu tähän resurssiin suojauspinnassa?
- Miten paketti yrittää päästä käsiksi resurssiin? (Mt.)

Kun politiikat rakennetaan siten, että ne vastaavat näihin kysymyksiin, voidaan saavuttaa Zero Trust -arkkitehtuurin mukainen liikenteen autentikointi. Kysymysten suuresta määrästä johtuen Zero Trust -politiikat ovat luonteeltaan huomattavasti hienojakoisempia perinteisten tietoturvaratkaisujen politiikkoihin verrattuna, joten verkkoliikenteen valvonta on oletusarvoisesti erittäin tarkkaa. (Mt.)

Kun Zero Trust -arkkitehtuurin mukainen verkko on otettu käyttöön onnistuneesti, sen toimintaa voidaan kehittää ja optimoida aktiivisella monitoroinnilla ja ylläpidolla. Arkkitehtuurin toimintaperiaate vaatii jatkuvaa ja toistuvaa autentikointia. Verkon kehittämisen kannalta on tärkeää, että kaikki organisaation verkossa tapahtuva liikenne dokumentoidaan tarkasti, jotta politiikat voidaan määritellä mahdollisimman tarkasti. (Mt.)

4.1.2 Hallinta- ja datapinta

Hallinta- ja datapinta eli Control Plane ja Data Plane ovat olennaisia käsitteitä Zero Trust -arkkitehtuurissa, ja niiden erilainen vuorovaikutustapa onkin yksi suurimmista eroista perinteisiin tietoturva-arkkitehtuureihin verrattuna. Hallinta- ja datapinta ovat jatkuvassa vuorovaikutuksessa toistensa kanssa, mutta Zero Trust -arkkitehtuuriin perustuvassa verkossa vuorovaikutuksen merkitystä korostetaan entisestään, koska liikenteen autentikointi tapahtuu arkkitehtuurin toimintaperiaatteen mukaisesti jatkuvasti. (Gilman & Barth 2017.)

Organisaation verkossa kaikki hallintapinnan ulkopuolella olevat asiat luokitellaan datapinnaksi. Hallintapinnan tehtävänä on nimensä mukaisesti hallita datapinnassa kulkevaa liikennettä määriteltyjen politiikkojen, sääntöjen ja Zero Trust -arkkitehtuurin periaatteiden mukaisesti. Datapinnasta lähetetään pyyntöjä hallintapinnalle, ja hallintapinnassa toimivat tietoturvatyökalut autentikoivat pyynnön lähettäneen käyttäjän sekä laitteen, joka käyttäjällä on pyyntöä lähettäessä käytössä. (Mt.)

Zero Trust -arkkitehtuurissa politiikat ja säännöt eroavat perinteisistä tietoturva-arkkitehtuureista siten, että ne ovat dynaamisia. Dynaamiset politiikat ja

niiden toimeenpano on reaaliaikaista, ja ne ottavat huomioon verkossa kulkevan liikenteen huomattavasti tarkemmin perinteisiin, staattisiin politiikkoihin verrattuna. Dynaamisuus mahdollistaa Zero Trust -arkkitehtuurin periaatteiden noudattamisen käytännössä, mutta vaatii myös uusia työkaluja. (Mt.)

Yksi Zero Trust -arkkitehtuurin käyttöönottoon liittyvistä haasteista onkin dynaamisten politiikkojen jatkuvan päivittämisen mahdollistaminen. Manuaalisesti tehtynä tehtävä on mahdoton, mutta verkkolaitteiden teknologian kehityksen myötä prosessi on mahdollista automatisoida esimerkiksi niin kutsuttuja uuden sukupolven palomuureja käyttämällä. Laitteet voivat myös hyödyntää koneoppimista ja tekoälyä dynaamisten politiikkojen päivittämisessä. (Mt.)

5 ZERO TRUST -ARKKITEHTUURIN MAHDOLLISTAJAT

5.1 Mikrosegmentointi

Verkon segmentointi on olennainen osa jokaista verkkoarkkitehtuuria. Organisaation sisäverkko voidaan segmentoida esimerkiksi siten, että yrityksen eri työtehtävissä oleville työntekijöille voidaan antaa käyttöoikeudet pelkästään tarvittaville alueille sisäverkossa. Yleisiä verkon segmentoinnin keinoja ovat esimerkiksi virtuaaliset lähiverkot (VLAN) ja pääsylistat (ACL). Perinteisen segmentoinnin ongelmana on sen karkeus, eli segmentoidut alueet ovat useimmiten tietoturvan kannalta liian laajoja, ja alueiden jakaminen liian pienikokoisiin osiin edellä mainittuja menetelmiä käyttämällä voi tehdä verkon ylläpitämisestä haastavaa. (Bednarz 2018.)

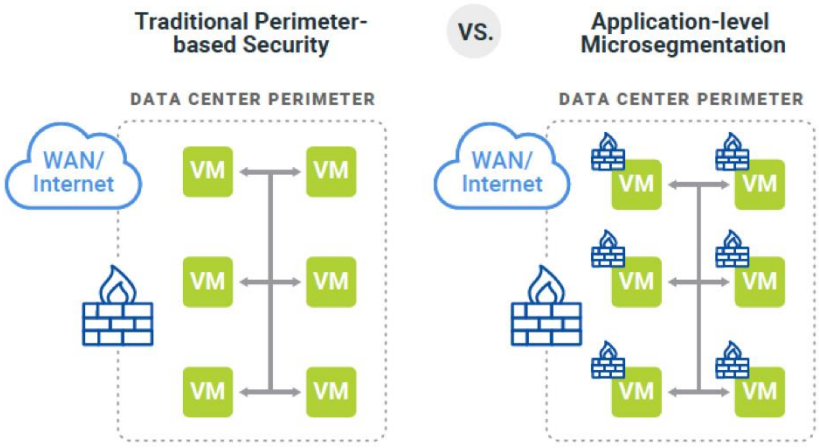
Mikrosegmentointi on nimensä mukaisesti hienojakoisempaa perinteiseen segmentointiin verrattuna. Tässä kontekstissa hienojakoisuudella tarkoitetaan tietoturvapolitiikkojen määrittelemistä esimerkiksi verkossa käytettävien laitteiden ja sovellusten perusteella. Mikrosegmentointi tapahtuu OSI-mallin 7. kerroksessa eli sovelluskerroksessa, jossa hienojakoisuus voi ulottua jopa yksittäisiin sovelluksiin. Hienojakoisuuden vuoksi on tärkeää, että organisaation sisäverkon rakenne on dokumentoitu tarkasti. Mikrosegmentoinnin yksityiskohtaisesta luonteesta johtuen sen implementoiminen voi olla haasteellista, jos organisaatiossa ei tiedetä, mitä laitteita ja sovelluksia verkossa on. (Mt.)

5.2 Virtualisointi ja mikrosegmentointi

Uuden sukupolven palomuureja voidaan käyttää organisaation verkon mikrosegmentointiin. Organisaatiossa saattaa olla laitteita, joiden ei tarvitse keskustella muiden kuin samaa tyyppiä olevien laitteiden kanssa, ja palomuurien politiikat voidaan määritellä siten, että nämä laitteet eivät kykene liikennöimään muualle kuin verkon toiminnan kannalta välttämättömiin kohteisiin. Organisaation verkon hyökkäyspinta pienenee merkittävästi, kun hakkerit eivät voi käyttää vähäpätöisempiä laitteita portteina verkon muihin osiin. (Mt.)

Erilaisten laitteiden ja sovellusten määrän kasvaessa myös palomuurien työkuorma kasvaa. Perinteiset palomuurit kykenevät määrittelemään sovelluskerroksen politiikkoja vain rajoitetusti. Mikrosegmentoidussa verkossa myös palomuurit segmentoidaan tarpeen mukaan, jolloin niiden määrä moninkertaistuu perinteiseen tietoturva-arkkitehtuuriin verrattuna. Fyysisiä palomuureja ei ole järkevää lisätä, koska taloudelliset kustannukset nousisivat kohtuuttomiin lukemiin. Tämän lisäksi politiikoilla ja säännöillä tulisi olla kyky muuttua dynaamisesti organisaation verkon tarpeiden mukaisesti. (Mt.)

Politiikkojen dynaamisuus on mahdotonta saavuttaa pelkästään fyysisiä palomuureja käyttämällä, koska ne eivät liiku verkossa olevien laitteiden mukana. Virtualisoinnin avulla palomuurien määrää voidaan kasvattaa kustannustehokkaasti ja niitä voidaan ylläpitää keskitetysti. Koska virtuaaliset palomuurit eivät ole sidoksissa mihinkään yksittäiseen sijaintiin, ne voivat liikkua organisaation verkossa tarpeen mukaan. (Mt.)



Kuva 4. Mikrosegmentoituja palomuureja (HyperConverged.org s.a.)

5.3 Monitasoinen autentikointi

Yksi teknologioista, joka tukee Zero Trust -arkkitehtuurin periaatteita, on monitasoisen autentikoinnin eli MFA:n (Multi Factor Authentication) käyttäminen. Monitasoista autentikointia käytettäessä käyttäjältä vaaditaan kirjautumisen yhteydessä käyttäjänimen ja salasanan lisäksi vähintään yhden toisenlaisen autentikointimenetelmän käyttäminen käyttöoikeuksien todentamiseksi. Monitasoinen autentikointiteknologia on kehitetty perinteisten autentikointimenetelmien rinnalle, koska pelkillä salasanoilla toteutettu autentikointi on todettu riittämättömäksi moderneja tietoturvauhkia vastaan. (Sundh 2017.)

5.3.1 Salasanojen ongelmat

Useamman autentikointimenetelmän käyttäminen on huomattavasti turvallisempaa pelkkään käyttäjänimeen ja salasanaan verrattuna, koska salasanat voivat joutua helposti vääriin käsiin inhimillisten virheiden takia. Salasanojen monimutkaisuusvaatimukset voivat jopa vähentää verkon tietoturvallisuutta, koska liian vaikeasti muistettavia salasanoja kirjoitetaan ylös turvattomiin sijainteihin, esimerkiksi tietokoneen vieressä oleville muistilapuille tai huomattavasti heikommin suojatuille alueille organisaation verkon sisällä, kuten käyttäjän työpöydällä olevaan tekstitiedostoon. (Mt.)

Osa salasanoista saattaa olla yhteisiä kaikille palvelun käyttäjille, jolloin on vaikeaa arvioida, kenellä käyttäjistä kuuluisi olla käyttöoikeudet ja kenellä ei. Vaikka salasanat olisivatkin ainoastaan käyttäjän omassa muistissa, se ei sulje pois tietojenkalastelusta aiheutuvia uhkia. Tietoturvallisesti säilytetty ja monimutkaisuuden kriteerit täyttävä salasana voi päätyä samalla tavalla vääriin käsiin kuin heikompi salasana. (Mt.)

5.3.2 Monitasoisen autentikoinnin työkalut

Monitasoinen autentikointi ei ole pelkästään Zero Trust -arkkitehtuuria varten luotu konsepti. Sitä on käytetty jo pitkään esimerkiksi käteisen noston yhteydessä pankkiautomaatilla: yksi osa tunnistautumista on käyttäjän hallussa oleva pankkikortti ja toinen osa on käyttäjän muistissa oleva PIN-koodi. Myös verkkopankkeihin kirjautuessa käytetään käyttäjänimen ja salasanan lisäksi

jonkinlaista käyttäjällä fyysisesti hallussa olevaa avainlukulistaa turvallisuuden lisäämiseksi. Näitä menetelmiä käyttämällä pelkkä käyttäjänimen ja salasanan varastaminen ei riitä käyttöoikeuksien kaappaamiseksi. (NIST 2016.)

Monitasoista autentikointia voidaan hyödyntää missä tahansa kirjautumista vaativassa palvelussa, eli käytännössä jokaisessa organisaation verkon osassa, joka on suojattu salasanalla, oli kyseessä sitten yksittäinen tiedosto tai kokonainen järjestelmä. Käytettävät menetelmät voivat hyödyntää esimerkiksi käyttäjän henkilökohtaisia ominaisuuksia tai fyysisesti hallussa olevia laitteita, kuten muistitikkuja ja älylaitteita.

Käyttäjällä fyysisesti hallussa oleva laite voidaan valjastaa monitasoisen autentikoinnin työkaluksi. Esimerkiksi muistitikkuun voidaan asentaa tunniste, joka vaaditaan kirjautumisen yhteydessä. Vaikka käyttäjän salasana olisi päätynyt vääriin käsiin, niin luvaton kirjautuminen ei onnistuisi ilman muistitikkua. Täysin ongelmaton ratkaisu ei ole, koska käyttäjä saattaa unohtaa kantaa laitetta mukanaan tai kadottaa sen, jolloin kirjautuminen ei onnistu.

Inhimillisistä virheistä johtuvat ongelmat voidaan välttää käyttämällä autentikointiin laitteita, jotka ovat käyttäjällä pääsääntöisesti aina mukana. Monet autentikointiratkaisut käyttävät älypuhelimeen ladattavaa sovellusta, joka generoi uuden avaimen tietyllä intervallilla, esimerkiksi minuutin välein. Ihmisten henkilökohtaiset ominaisuudet ovat pääsääntöisesti aina käytettävissä, joten sormenjälkiä ja muita biometrisiä ominaisuuksia voidaan hyödyntää myös autentikoinnissa, kunhan autentikoinnin vastaanottava laite kykenee tulkitsemaan biometrisiä tietoja. Sormenjäljenlukija kuuluu monien nykyaikaisten kannettavien tietokoneiden ja älylaitteiden perusvarusteluun.

Edellä mainittuja työkaluja voidaan käyttää samanaikaisesti vaihtoehtoisina menetelminä, jolloin autentikointi ei epäonnistu inhimillisten erehdyksien takia. Organisaation verkon kriittisimmät alueet voidaan suojata päällekkäisillä autentikointimenetelmillä, mutta autentikointi tulisi säilyttää suhteellisen vaivattomana hyvän käyttäjäkokemuksen ylläpitämiseksi.

5.4 Julkisten avainten hallintajärjestelmä

Vaikka Zero Trust -arkkitehtuurin tarkoituksena on luottamuksen poistaminen, niin arkkitehtuuriin perustuvassa verkossa voidaan soveltaa luottamukseen perustuvia teknologioita, joista yksi on julkisten avainten hallintajärjestelmä eli PKI (Public Key Infrastructure). PKI on autentikointimenetelmä, jossa sekä käyttäjä että kirjautumisen kohteena oleva verkko luottavat samaan tahoon, joka lähettää digitaalisen sertifikaatin käyttäjälle, laitteelle tai palvelulle. Tämä sertifikaatti toimii avaimena verkkoon, ja koska myös kohteena oleva verkko kommunikoi sertifikaatin myöntäjän kanssa, sen oikeellisuus voidaan vahvistaa autentikointia vaativan tahon toimesta. (Gilman & Barth 2017, 59–61.)

5.4.1 Varmentaja

Varmentaja eli CA (Certificate Authority) on taho, joka myöntää digitaalisen sertifikaatin käyttäjälle ja vahvistaa sen oikeellisuuden. Vastuu sertifikaattien myöntämisestä voidaan luovuttaa kolmannen osapuolen yrityksille, mutta Zero Trust -arkkitehtuuriin perustuvassa verkossa organisaation yksityinen varmentaja noudattaisi arkkitehtuurin periaatteita paremmin. Kolmannen osapuolen hallinnoima hallintajärjestelmä on kuitenkin tyhjää parempi vaihtoehto. (Mt.)

Yksityinen julkisten avainten hallintajärjestelmä eli Private PKI toimii samalla periaatteella kuin kolmannen osapuolen PKI, mutta hallintajärjestelmä on kokonaan organisaatiolla itsellään. Yksityisen varmentajan implementoimisessa ja ylläpitämisessä on omat haasteensa, mutta organisaatio voi kustomoida omassa omistuksessa olevaa hallintajärjestelmää tehokkaammin eivätkä sertifikaatit ole riippuvaisia kolmannesta osapuolesta. Lisäksi se on useimmiten taloudellisesti kannattavampaa, koska Zero Trust -arkkitehtuuriin perustuvassa verkossa käytetään useita erilaisia sertifikaatteja, ja sertifikaattien määrän kasvaessa myös yritysten tarjoamien palvelujen hinnat nousevat. (Mt.)

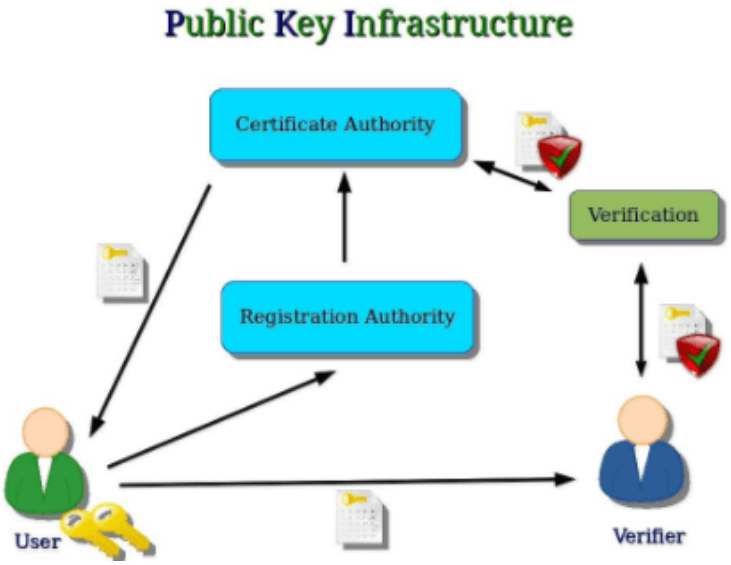
5.4.2 Rekisteröijä

Rekisteröijä eli RA (Registration Authority) on PKI-hallintajärjestelmän osa, jonka tehtävänä on vastaanottaa käyttäjiltä, laitteilta ja palveluilta tulevat pyyn-

nöt digitaalisia sertifikaatteja koskien. Rekisteröijä myös suorittaa hallintajärjestelmän sisäisen autentikoinnin, jotta sertifikaatit eivät päädy vääriin käsiin. Mikäli pyynnön lähettäjän oikeellisuus todennetaan onnistuneesti, rekisteröijä lähettää pyynnön eteenpäin varmentajalle. (The Security Buddy 2017.)

5.4.3 Vahvistaja

Vahvistaja eli VA (Verification Authority) on autentikointia vaativan verkon taho, joka kommunikoi varmentajan kanssa vahvistaakseen vastaanotettavien sertifikaattien oikeellisuuden. Kun sertifikaatille annetaan viimeinen vahvistus, niin autentikointi on valmis. (Mt.)



Kuva 5. PKI:n toimintaperiaate (The Security Buddy 2017)

5.5 Uuden sukupolven palomuurit

Uuden sukupolven palomuuri eli NGFW (Next Generation Firewall) on nimensä mukaisesti perinteistä palomuuria kehittyneempi tietoturvatyökalu, jonka tulisi sisältää ICT-alan tutkimus- ja konsultointiyritys Gartnerin mukaan ainakin seuraavat ominaisuudet:

- Tavallisen palomuurin ominaisuudet, kuten tilallinen tarkastelu.
- Integroitu tunkeutumisen torjuminen.
- Sovellustietoisuus, kyky nähdä ja estää riskialttiita sovelluksia.
- Kyky hyödyntää lähteitä tietoturvauhista.
- Kyky päivittyä vastaamaan tulevaisuuden tarpeita.
- Valmius puolustautua kehittyviä uhkia vastaan. (Cisco s.a.)

Yksi Zero Trust -arkkitehtuurin mahdollistajista on verkon mikrosegmentointi, joka voidaan suorittaa esimerkiksi uuden sukupolven palomuurien ominaisuuksia hyödyntämällä. Mikrosegmentoinnissa käytetään useimmiten sekä fyysisiä että virtuaalisia palomuureja, koska virtualisoinnin avulla suurikin määrä palomuureja on ylläpidettävissä ja kustannukset ovat huomattavasti matalampia fyysisiin laitteisiin verrattuna. (Palo Alto Networks s.a.)

5.6 Verkkosovelluspalomuurit

Zero Trust -arkkitehtuurille olennaista sovelluskerroksen tietoturvaa voidaan parantaa verkkosovelluspalomuureilla eli Web Application Firewall -laitteilla (WAF). Verkkosovelluspalomuuriratkaisut voivat olla perinteisten palomuurien kaltaisia fyysisiä laitteita, jotka keskittyvät verkkopohjaisiin sovelluksiin kohdistettujen hyökkäyksien, kuten SQL-injektioiden ehkäisemiseen. Palomuuri voidaan myös integroida osaksi sovellusta. (Cloudflare s.a.)

Verkkosovelluspalomuureilla voidaan saavuttaa Zero Trust -arkkitehtuurin vaatima politiikkojen ja sääntöjen hienojakoisuus, koska kehittyneiden verkkosovelluspalomuurien työkalut kykenevät suojaamaan verkkosovellusten eri osia, mikä lisää sovelluksen turvallisuutta huomattavasti. (Mt.)

6 ZERO TRUST -ARKKITEHTUURIN ONGELMAT

Vaikka Zero Trust -arkkitehtuurilla pyritään ratkaisemaan monia perinteisille tietoturva-arkkitehtuureille tyypillisiä perustavanlaatuisia ongelmia, niin kyseessä ei ole täysin aukoton ratkaisu, ja muiden arkkitehtuurien tavoin myös Zero Trust -ratkaisut ovat saaneet kritiikkiä osakseen. Suurimmiksi ongelmiksi on havaittu arkkitehtuurin potentiaalisesti haastava implementointi ja liiallisen luottamattomuuden tuomat ongelmat. (Haber 2019.)

6.1 Vanhat ohjelmistot

Zero Trust -arkkitehtuurin implementoiminen voi olla haasteellista, jos organisaation olemassa olevaa verkkoa aiotaan uudistaa arkkitehtuurin mukaiseksi ja lähtökohdat ovat heikot. Suurilla organisaatioilla voi olla käytössään satoja, ellei jopa tuhansia resursseja, joiden tulisi noudattaa Zero Trust -periaatteita.

Periaatteiden mukaisten politiikkojen ja sääntöjen määrittely voi olla pitkä tai jopa mahdoton prosessi, koska monilla yrityksillä on käytössä vanhoja ohjelmistoja, jotka eivät välttämättä kykene taipumaan näiden periaatteiden asettamiin vaatimuksiin. Jos vanhan ohjelmiston ainoa saatavilla oleva autentikointimenetelmä on käyttäjätunnus ja salasana, niin modernien tietoturvatyökalujen lisääminen voi olla epäkäytännöllistä. (Mt.)

6.2 Vertaisverkot

Vertaisverkkojen eli P2P-teknologian käyttäminen aiheuttaa yhteensopivuusongelmia Zero Trust -arkkitehtuuriin perustuvissa verkoissa. P2P-teknologiaa käytettäessä verkon päätelaitteet toimivat sekä palvelimina että asiakkaina, ja kykenevät keskustelemaan keskenään ilman välikäsiä verkon sisällä. Zero Trust -arkkitehtuuriin perustuvissa verkoissa hallintapinnassa sijaitseva taho hallitsee ja valvoo verkossa kulkevaa liikennettä. Tämän periaatteen takia P2P-teknologian käyttäminen on mahdotonta. Teknologioiden poissulkeminen heikentää arkkitehtuurin joustavuutta. (Mt.)

6.3 Kustannukset

Zero Trust -arkkitehtuurin käyttöönoton kustannukset riippuvat organisaation verkon laajuudesta ja käytettävästä teknologiasta. Tietoturvaratkaisuja tarjoavien yritysten Zero Trust -implementaatiot noudattavat samoja periaatteita, mutta menetelmät arkkitehtuurin saavuttamiseksi voivat poiketa valmistajakohtaisesti, mikä vaikuttaa myös ratkaisujen kustannuksiin. Esimerkiksi uuden sukupolven palomuurien hinnat voivat vaihdella ominaisuuksista riippuen 1 000 eurosta yli 100 000 euroon (SecureITStore.com s.a.).

Joissakin tapauksissa olemassa olevan verkon arkkitehtuurin vaihtamiseen liittyvät muutostyöt voivat kustantaa enemmän kuin alusta alkaen rakennettu Zero Trust -arkkitehtuuriin perustuva verkko. Edellä mainitut kompastuskivet voidaan välttää alusta alkaen implementoitavissa ratkaisuissa, koska organisaatiossa käytettävien ohjelmistojen ja verkossa käytettävien laitteiden valintaprosessissa voidaan tällöin huomioida Zero Trust -arkkitehtuurin tarpeet.

Vaikka Zero Trust -arkkitehtuuri on teoriassa mahdollista implementoida osaksi olemassa olevaa verkkoa, niin muutoksen kohteena olevan yrityksen tulee pohtia, mitä muutoksia nykyiseen verkkoinfrastruktuuriin on tehtävä, jotta arkkitehtuuri voidaan ottaa käyttöön onnistuneesti. Toimiva kokonaisuus vaatii tarkkaa dokumentaatiota verkon eri osista ja niihin liittyvistä käyttöoikeuksista. Tuhansien ohjelmistojen ja palvelujen läpikäyminen näiden käyttöoikeuksien määrittämiseksi voi olla aikaa vievä prosessi, mikä kasvattaa kustannuksia.

7 ESIMERKKEJÄ ZERO TRUST -RATKAISUISTA

7.1 Google – BeyondCorp

BeyondCorp on Google-yhtiön projekti, jossa noudatetaan tietoturvan osalta Zero Trust -arkkitehtuurin toimintaperiaatteita. Projekti syntyi aloitteesta, jonka päämääränä oli mahdollistaa työntekijöiden työskentely organisaation sisäverkkojen ulkopuolella ilman VPN-yhteyttä, tietoturvaa vaarantamatta. Tänä päivänä BeyondCorp on käytössä suurimmalla osalla Googlen työntekijöistä. Projekti on kasvanut yhdeksi tunnetuimmista Zero Trust -ratkaisuista, ja se on rakennettu seuraavien periaatteiden pohjalle:

- Tietystä verkosta yhdistäminen ei riitä käyttöoikeuksien jakamiseksi käyttäjälle.
- Käyttöoikeudet jaetaan sen perusteella, mitä yhdistävästä käyttäjästä ja päätelaitteesta tiedetään.
- Käyttöoikeuksien jakaminen täytyy olla autentikoitua, auktorisoitua ja salattua. (Google s.a.)

7.2 ZeroTier

ZeroTier on avoimeen lähdekoodiin perustuva palvelu, jonka toimintaperiaate on saanut inspiraatiota muun muassa BeyondCorp-ratkaisusta. Palvelu on mahdollista ottaa käyttöön yleisimmissä käyttöjärjestelmissä, kuten Windows, MacOS ja erilaiset Linux-käyttöjärjestelmät. Mobiilikäyttöjärjestelmistä Apple iOS ja Android ovat myös vaihtoehtoja. (ZeroTier s.a.)

Avoimeen lähdekoodiin perustuvana ohjelmistona ZeroTier on käytettävissä ilmaiseksi, eikä sen käytöstä tarvitse maksaa lisenssimaksuja, jos palvelua käytetään voittoa tuottamattomiin projekteihin. ZeroTier-palvelu valittiin tämän

opinnäytetyön käytännön osiossa käytettäväksi ratkaisuksi, koska palveluun liittyvät ohjelmistot ovat yhteensopivia monien laitteiden kanssa ja palvelun käyttäminen kokeellisissa tutkimuksissa on maksutonta. (Mt.)

7.3 ZeroTier-palvelun toimintaperiaate

ZeroTier-palvelu on virtualisointityökalu, jonka tavoitteena on yhdistää kaikki organisaation verkon resurssit yhdeksi kokonaisuudeksi. ZeroTier-palvelun kehittäjät kuvailevat palvelua eräänlaiseksi “koneiden keskusteluhuoneeksi”. Yksinkertaisesti selitettynä palvelu otetaan käyttöön luomalla virtuaalinen verkko, johon yhdistetään halutut resurssit. Näihin resursseihin liittyviä käyttöoikeuksia voidaan määritellä hienojakoisesti palvelun tarjoamilla tietoturvatyökaluilla ja kolmannen osapuolen palomuureilla. (ZeroTier s.a.)

7.3.1 Liikenteen kulkeminen

ZeroTier-palvelua käyttämällä saavutetaan samankaltainen lopputulos kuin VPN-teknologialla, mutta tietyt asiat erottavat nämä kaksi palvelua toisistaan. VPN-palvelun toimintaperiaatteena on luoda tunneli kahden verkon välille, esimerkiksi etätyöntekijän kotiverkosta organisaation sisäverkkoon. (Mt.)

ZeroTier tuo etätyöntekijän tietokoneen osaksi organisaation verkkoa samalla tavalla kuin uusi laite liitettäisiin sisäverkossa sijaitsevan kytkimen porttiin. Palvelussa perinteisen sisäverkon päällä toimii virtuaalinen ZeroTier-verkko, joka hallitsee yhteyksiä, oli kyseessä sitten sisäverkon resurssien välinen liikennöinti tai etäyhteys. ZeroTier-palvelua voidaankin pitää pilvessä sijaitsevana, älykkäänä kytkimenä. (Mt.)

Yhteyden muodostaminen ZeroTier-verkoissa tapahtuu palvelun tarjoamien juuripalvelimien välityksellä. Verkot ovat riippuvaisia näiden juuripalvelimien toiminnasta, mutta myös yksityisten juuripalvelimien rakentaminen on mahdollista. Yksityisten juuripalvelimien avulla sisäverkkoon saadaan redundanttisuutta, ja verkko jatkaa toimintaansa, vaikka yhteys ZeroTier-juuripalvelimiin katkeaisi. Liikenne suojataan 256-bittisellä Curve25519-salauksella. (Mt.)

7.3.2 UDP Hole Punching

ZeroTier-verkoissa laitteet muodostavat yhteyden toisiinsa käyttämällä UDP Hole Punching -teknologiaa, joka on yleisesti käytetty keino kulkea osoitteenmuunnoksen (NAT) läpi. Teknologiassa kaksi laitetta liikennöi keskenään, mutta ensimmäinen yhteys muodostetaan yhteisen kolmannen osapuolen välityksellä. ZeroTier-palvelu on tämä kolmas osapuoli. Jos yhteyden molemmat osapuolet käyttävät symmetristä osoitteenmuunnosta (Symmetric NAT), niin UDP Hole Punching -teknologia ei toimi luotettavasti, koska yhteyksissä käytettävät portit vaihtuvat satunnaisesti. (ZeroTier 2014.)

7.4 Palvelun edut

ZeroTier on suhteellisen helppokäyttöinen palvelu yksinkertaisella graafisella käyttöliittymällä. Yksinkertaisen verkon luominen on nopea prosessi, ja uusien yhteyksien muodostaminen toimii nopeasti. Suurempien verkkojen ylläpitäminen voi osoittautua haasteelliseksi manuaalisesti tehtynä, mutta palvelun käyttöönottoa ja ylläpitämistä on mahdollista automatisoida API-rajapinnalla.

Zero Trust -arkkitehtuurin tarpeet on otettu huomioon kehittyneillä tietoturvatyökaluilla. ZeroTier-palvelun Flow Rules -osiossa voidaan määritellä tarkkoja politiikkoja ja sääntöjä. joiden avulla Zero Trust -arkkitehtuurin mukaiset periaatteet ovat saavutettavissa. Verkossa kulkevaa liikenteen tarkan rajaamisen lisäksi kaikki liikenne voidaan kopioida esimerkiksi uuden sukupolven palomuurin tarkasteltavaksi. Tätä menetelmää käyttämällä myös sisäverkossa olevia uhkia voidaan analysoida ja ehkäistä.

ZeroTier-palvelun käyttäminen yleisimmissä verkoissa on maksutonta, joten se voi osoittautua edullisimmaksi ratkaisuksi, kun organisaatiossa pohditaan erilaisten etäyhteys- ja tietoturvaratkaisujen kustannuksia.

7.5 Palvelun ongelmat

Zero Trust -arkkitehtuurin kannalta ZeroTier-palvelun ongelmaksi muodostuu pakollinen luottamus palveluntarjoajaan. ZeroTier-juuripalvelimet ovat välttämättömiä yhteyksien muodostamiseksi, mutta yksi Zero Trust -arkkitehtuurin oletusarvoista on se, että kolmannen osapuolen tahoihin ei luoteta.

Palvelua voidaan pitää Zero Trust -arkkitehtuurin hallintapintana, mutta hallintapinnan tulisi olla täysin organisaation verkon hallussa. Yksityinen juuripalvelin ratkaisee tämän ongelman osittain, mutta sisäverkon ulkopuoliset yhteydet vaativat palvelun omia juuripalvelimia.

ZeroTier-palveluun kirjautuminen tapahtuu tällä hetkellä pelkän käyttäjänimen ja salasanan perusteella. Opinnäytetyössä on käsitelty salasanoihin liittyviä ongelmia, ja koska ZeroTier ei tue esimerkiksi monitasoista autentikointia, niin se muodostaa heikon lenkin organisaation verkon tietoturvallisuuteen. Jos palvelun salasana joutuu vääriin käsiin, hyökkääjä voi muuttaa verkon käyttöoikeuksia ja politiikkoja mielivaltaisesti.

8 ZERO TRUST -ARKKITEHTUURIN IMPLEMENTOINTI

Käytännön osion tavoitteena on rakentaa yksinkertainen verkko virtuaaliseen laboratorioympäristöön ja tutkia, kuinka Zero Trust -arkkitehtuurin periaatteita voidaan implementoida osaksi verkkoa ZeroTier-palvelun tarjoamia työkaluja käyttämällä. Verkko ja siihen liittyvät palvelut rakennetaan Kaakkois-Suomen ammattikorkeakoulun kehittämälle VirtualLab-laboratorioympäristölle, joka mahdollistaa verkon simuloimisen ilman fyysisiä laitteita. Käytännön osio voidaan luokitella soveltuvuusselvitykseksi, jonka tavoitteena on tutkia, voiko Zero Trust -arkkitehtuuriin perustuvia työkaluja hyödyntää VirtualLab-alustalla.

Käytännön osio on toteutettu ohjeen muodossa, joka on luettavissa tämän opinnäytetyön liiteessä (liite 1). Ohjeessa käydään läpi ZeroTier-palvelun käyttöönottaminen VirtualLab-alustalla vaihe vaiheelta. Koska ohjeen aiheena on pääasiallisesti ZeroTier-palvelu, siinä ei käsitellä aiheen kannalta epäolennaisia asioita yksityiskohtaisesti, ja ohjetta noudattavalla henkilöllä olisi hyvä olla osaamista tietoliikenneteknologiasta ja VirtualLab-alustasta.

Ohje perustuu ZeroTier-palvelun viralliseen dokumentaatioon (ZeroTier s.a) ja Óscar Amorin ohjeistukseen ZeroTier-palvelun implementoinnista OpenWrt-käyttöjärjestelmässä (Amor 2019).

9 LOPPUTULOS

Opinnäytetyössä tutkittiin Zero Trust -arkkitehtuuria ja sen toimintaperiaatetta sekä teoriassa että käytännössä. Teoriaosiossa tutustuttiin arkkitehtuurin historiaan ja esiteltiin arkkitehtuurin toimintaperiaatetta. Arkkitehtuuria verrattiin perinteisiin tietoturva-arkkitehtuureihin, ja opinnäytetyössä selitettiin erilaisten arkkitehtuurien hyviä ja huonoja puolia. Yleisen toimintaperiaatteen lisäksi opinnäytetyössä tutkittiin Zero Trust -arkkitehtuurin mahdollistavia konsepteja ja teknologioita, joiden toimintaperiaatteet selitettiin kattavasti.

Käytännön osion tavoitteena oli implementoida Zero Trust -arkkitehtuurin periaatteiden mukainen verkko VirtualLab-alustalle soveltuvuusselvityksenä. Osiossa onnistuttiin luomaan simuloitu verkko, jossa käytetään ZeroTier-palvelua. Palvelun tarjoamien ominaisuuksien lisäksi tutkittiin mahdollisia ongelmia, joita tulee ottaa huomioon VirtualLab-alustaa käytettäessä. Lopputuloksena syntyi ohje, jota voidaan käyttää pohjana Zero Trust -arkkitehtuuriin liittyvissä projekteissa, mikäli ratkaisua halutaan kehittää.

Opinnäytetyön johdannossa määriteltyihin Zero Trust -arkkitehtuuriin liittyviin tutkimuskysymyksiin vastattiin onnistuneesti, minkä perusteella voidaan todeta, että opinnäytetyö on toteutettu onnistuneesti.

Opinnäytetyön teoriaosioon perehtymällä voi muodostaa yleiskuvan Zero Trust -arkkitehtuurista, sen toimintaperiaatteesta ja siihen liittyvistä teknologioista. Käytännön osiota hyödyntämällä Zero Trust -arkkitehtuurin käyttöönotto ZeroTier-palvelulla ja VirtualLab-alustalla on helpompaa, koska konsepti on todettu toimivaksi ja opinnäytetyön liitteenä olevaa ohjeistusta soveltamalla monilta kompastuskiviltä voidaan välttyä tulevaisuuden kehitysprojekteissa.

Yksi kehitysmahdollisuuksista on ZeroTier-palvelun hyödyntäminen suuremmassa mittakaavassa. VirtualLab-alustalle voisi rakentaa esimerkiksi kopion

olemassa olevan yrityksen verkosta, ja tavoitteena voisi olla kyseisen verkon muuttaminen ZeroTier-palvelulla toimivaksi Zero Trust -kokonaisuudeksi.

Toisena kehityshankkeena voitaisiin tutkia muita Zero Trust -arkkitehtuurin periaatteisiin sopivia tietoturvatyökaluja, jotka voisivat toimia hyvin yhteistyössä ZeroTier-palvelun kanssa, kuten avoimen lähdekoodin palomuurit.

Kolmas kehityksen kohde on ZeroTier-palvelun käyttöönoton helpottaminen esimerkiksi automatisointia hyödyntämällä. Palveluun on saatavilla API, jota käyttämällä palvelun implementointiin ja ylläpitämiseen liittyviä toimenpiteitä on mahdollista automatisoida.

LÄHTEET

Amor, Ó. 2015. ZeroTier setup on OpenWRT. WWW-dokumentti. Päivitetty 26.4.2019. Saatavissa: https://github.com/mwarning/zerotier-openwrt/wiki [viitattu 31.1.2020].

Arbor Networks. 2017. DDoS Attack Types. PDF-dokumentti. Saatavissa: https://www.inforte.com/wp-content/uploads/2018/06/DDoS-ATTACK-TYPES.pdf [viitattu 19.1.2020].

Armon, D. 2018. The What, Why, and How of Zero Trust Networking. WWW-dokumentti. Saatavissa: https://www.hashicorp.com/resources/how-zero-trust-networking [viitattu 27.12.2019].

Barracuda. s.a. What is a DMZ Network? WWW-dokumentti. Saatavissa: https://www.barracuda.com/glossary/dmz-network [viitattu 21.12.2019].

Bednarz, A. 2018. What is microsegmentation? How getting granular improves network security. WWW-dokumentti. Saatavissa: https://www.networkworld.com/article/3247672/what-is-microsegmentation-how-getting-granular-improves-network-security.html [viitattu 14.1.2020].

Cisco. s.a. What Is a Next-Generation Firewall? WWW-dokumentti. Saatavissa: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html [viitattu 2.1.2020].

Cloudflare. s.a. What is a WAF? | Web Application Firewall explained. WWW-dokumentti. Saatavissa: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/ [viitattu 3.2.2020].

Cunningham, C. 2019. The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019. WWW-dokumentti. Saatavissa: https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+Ecosystem+Platform+Providers+Q4+2019/-/E-RES146875 [viitattu 18.12.2019].

Gilman, E. & Barth, D. 2017. Zero Trust Networks. WWW-dokumentti. Saatavissa: https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html [viitattu 19.12.2019].

Gilman, E. & Barth, D. 2017. Zero Trust Networks. 1. painos. Yhdysvallat: O'Reilly Media, Inc.

Google. s.a. BeyondCorp. WWW-dokumentti. Saatavissa: https://cloud.google.com/beyondcorp/ [viitattu 10.12.2019].

Haber, M. 2019. Why Zero Trust is an Unrealistic Security Model. WWW-dokumentti. Saatavissa: https://www.beyondtrust.com/blog/entry/why-zero-trust-is-an-unrealistic-security-model [viitattu 21.1.2020].

HyperConverged.com. s.a. How to Beef Up Your Hyperconverged Infrastructure Security With Microsegmentation. WWW-dokumentti: Saatavissa: https://www.hyperconverged.org/hyperconverged-infrastructure-security-micro-segmentation/ [viitattu 2.1.2020].

Internet World Stats. 2019. Internet Growth Statistics. WWW-dokumentti. Saatavissa: https://www.internetworldstats.com/emarketing.htm [viitattu 9.12.2019].

ISO/IEC 7498-1:en. 1994. Information technology. Open Systems Interconnection. Basic Reference Model: The Basic Model. Part 1. [viitattu 3.2.2020].

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä: Kehittämistutkimuksen kirjoittamisen käytännön opas. 1. painos. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Markets and Markets. 2019. Zero-Trust Security Market. WWW-dokumentti. Saatavissa: https://www.marketsandmarkets.com/Market-Reports/zero-trust-security-market-2782835.html [viitattu 18.12.2019].

Mitra, A. 2017. Public Key Infrastructure and Blockchain. WWW-dokumentti. Saatavissa: https://www.thesecuritybuddy.com/blockchain/public-key-infrastructure-and-blockchain/ [viitattu 3.1.2020].

NIST. 2016. Back to basics: Multi-factor authentication (MFA). WWW-dokumentti. Saatavissa: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication [viitattu 7.1.2020].

Palo Alto Networks. s.a. Implementing Zero Trust Using the Five-Step Methodology. WWW-dokumentti. Saatavissa: https://www.paloaltonetworks.com/cyberpedia/zero-trust-5-step-methodology [viitattu 30.12.2019].

Palo Alto Networks. s.a. What is Zero Trust? WWW-dokumentti. Saatavissa: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture [viitattu 29.12.2019].

Reuters. 2019. Yahoo strikes $117.5 million data breach settlement after earlier accord rejected. WWW-dokumentti. Saatavissa: https://www.reuters.com/article/us-verizon-yahoo/yahoo-in-new-117-5-million-data-breach-settlement-after-earlier-accord-rejected-idUSKCN1RL1H1 [viitattu 9.12.2019].

Risk Based Security. 2019. Data Breach QuickView Report. WWW-dokumentti. Saatavissa: https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report [viitattu 9.12.2019].

SecureITStore.com. s.a. Cisco Firepower Next-Generation Firewall. WWW-dokumentti. Saatavissa: https://www.secureitstore.com/Firepower-NGFW.asp [viitattu 21.1.2020].

Sundh, S. 2017. 13 reasons why passwords are not secure. WWW-dokumentti. Saatavissa: https://www.nexusgroup.com/why-passwords-not-secure/ [viitattu 5.1.2020].

Svobunas, A. 2017. Implementing a private cloud with System Center 2016 in a virtual lab environment. Kaakkois-Suomen ammattikorkeakoulu. Tieto- ja viestintätekniikka. Opinnäytetyö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:amk-201705056607 [viitattu 7.12.2019].

Varkama, S. 2017. MPLS Segment Routing Technology Study. Kaakkois-Suomen ammattikorkeakoulu. Tieto- ja viestintätekniikka. Opinnäytetyö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:amk-201705097047 [viitattu 7.12.2019].

Walkowski, D. 2019. What Is The CIA Triad? WWW-dokumentti. Saatavissa: https://www.f5.com/labs/articles/education/what-is-the-cia-triad [viitattu 16.12.2019].

ZeroTier. s.a. Manual. WWW-dokumentti. Saatavissa: https://www.zerotier.com/manual/ [viitattu 3.2.2020].

ZeroTier. 2014. The State of NAT Traversal. WWW-dokumentti. Saatavissa: https://www.zerotier.com/the-state-of-nat-traversal/ [viitattu 3.2.2020].

ZeroTier. s.a. ZeroTier. WWW-dokumentti. Saatavissa: https://www.zerotier.com/ [viitattu 30.1.2020].

ZeroTier. s.a. ZeroTier Knowledgebase. WWW-dokumentti. Saatavissa: https://zerotier.atlassian.net/wiki/spaces/SD/overview [viitattu 31.1.2020].

KUVALUETTELO

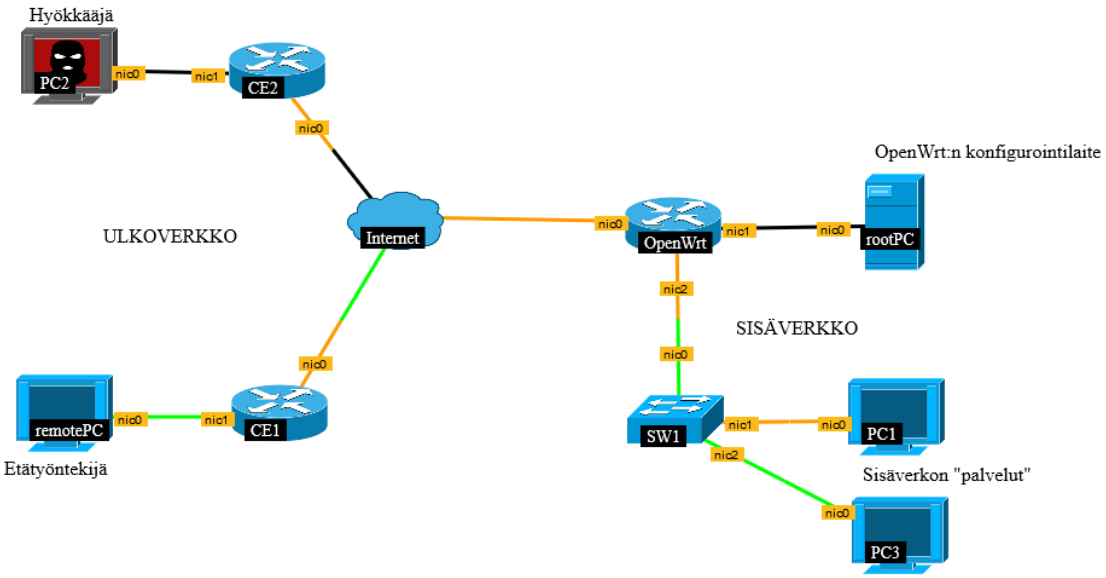
Liite 1/1

ZEROTIER-PALVELUN KÄYTTÖÖNOTTAMINEN

Tässä esimerkissä laboratorioon on rakennettu pieni sisäverkko ja ulkoverkko. Sisäverkon laitteet ”PC1” ja ”PC3” simuloivat palveluja, joihin käyttöoikeuksilla varustettujen käyttäjien tulisi päästä käsiksi. Palvelut ovat tässä tapauksessa Windows 7 -käyttöjärjestelmällä varustettuja tietokoneita, joiden tarkoituksena on vastata ping-kutsuihin käyttöoikeuksien tarkastamista varten. Nämä laitteet sijaitsevat kytkimen ”SW1” takana.

Laite ”OpenWrt” on sisäverkon reititin. OpenWrt on pääasiassa reititinkäyttöä varten kehitetty Linux-käyttöjärjestelmä, jossa on tuki ZeroTier-palvelulle. Tämä reititin toimii sisäverkon Internet-yhdyskäytävänä. Laite ”rootPC” toimii Debian 9 -käyttöjärjestelmällä, ja sen tehtävänä on hallita sisäverkon reititintä SSH-yhteyden välityksellä. Ulkoista konfigurointilaitetta käyttämällä myös graafisen käyttöliittymän hyödyntäminen on mahdollista.

Internet-yhteys luodaan toiminnolla ”Add Interconnection (MulticastVPN)”, ja toiminnon IP-osoitteeksi asetetaan 239.10.10.10. Laitteet ”CE1” ja ”CE2” ovat simuloidun etätyöntekijän ja hyökkääjän reitittimiä, jotka toimivat molempien päätelaitteiden Internet-yhdyskäytävinä. Laitteet ”remotePC” ja ”PC2” ovat Windows 7 -käyttöjärjestelmällä toimivia tietokoneita.



Kuva 6. VirtualLab-alustan topologianäkymä

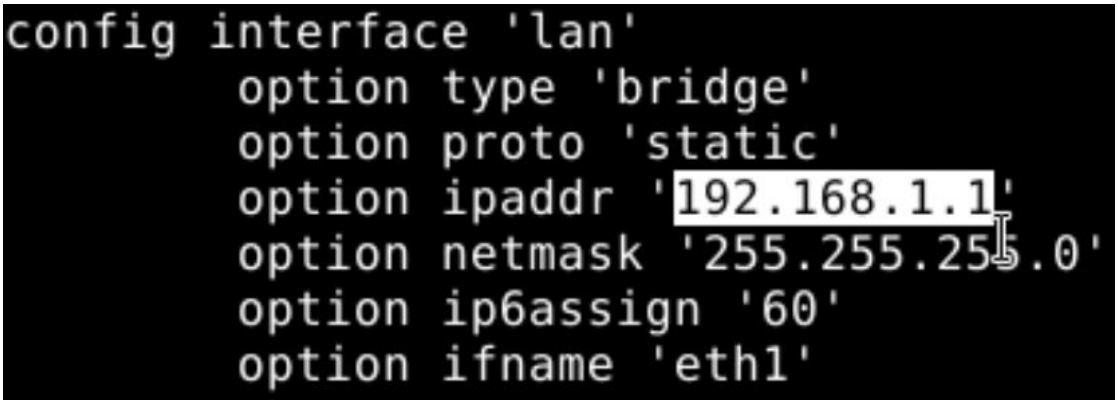
Internet-toiminto jakaa reunareitittimille IP-osoitteet osoiteavaruudesta 192.168.1.0/24. OpenWrt-laitteen hallintaosoite on oletuksena 192.168.1.1, joka on päällekkäisyyden takia vaihdettava. Vaihtoa ei voi tehdä graafisessa käyttöliittymässä, joten on muodostettava SSH-yhteys komentokehotteella.

Yhteyttä varten OpenWrt-laitteen salasana on vaihdettava komennolla:
 # *passwd*

SSH-yhteys muodostetaan laitteelta ”rootPC” komennolla:
 # *ssh 192.168.1.1*

Reitittimen hallintaosoitetta voi muuttaa esimerkiksi Nano-tekstieditorilla:
 # *nano /etc/config/network*

Osoite on vaihdettava toiseen osoiteavaruuteen, esimerkiksi 192.168.2.0/24. Kuvassa 6 on korostettu muutettavaa IP-osoitetta.

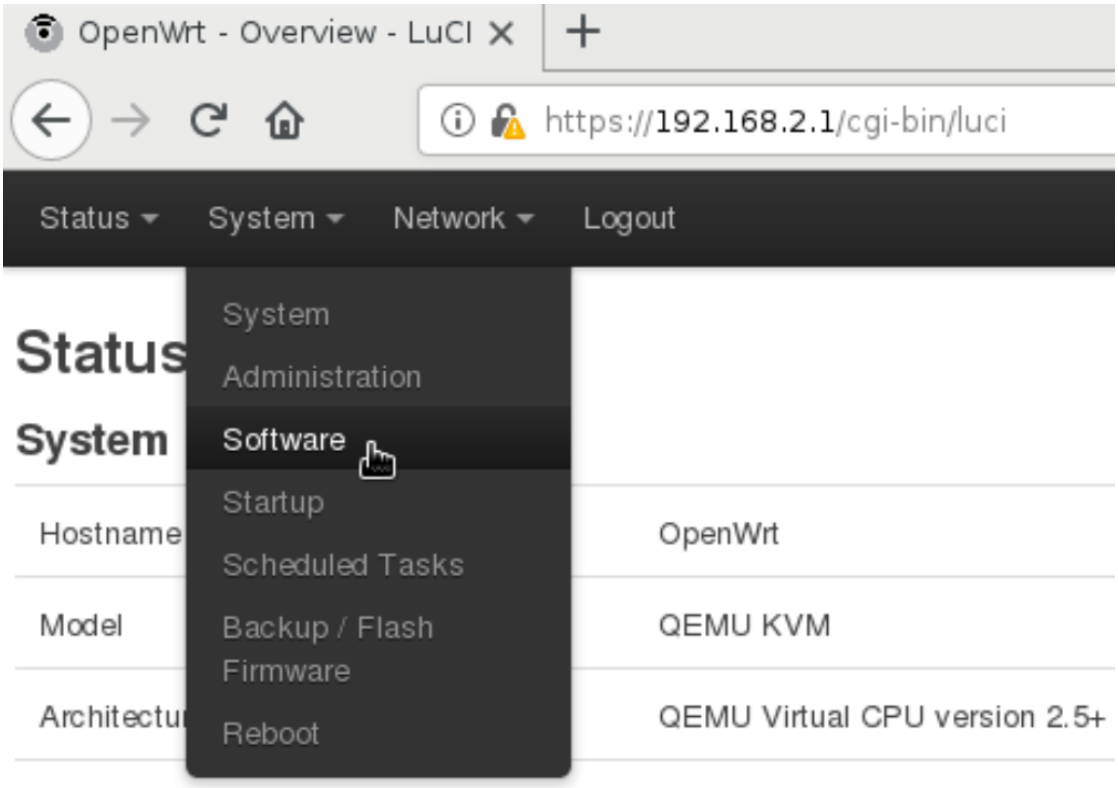


Kuva 7. Hallintaosoitteen muokkaaminen /etc/config/network -tiedostossa

Muutokset astuvat voimaan verkkopalvelun uudelleenkäynnistämisen jälkeen.
 # *letc/init.d/network restart*

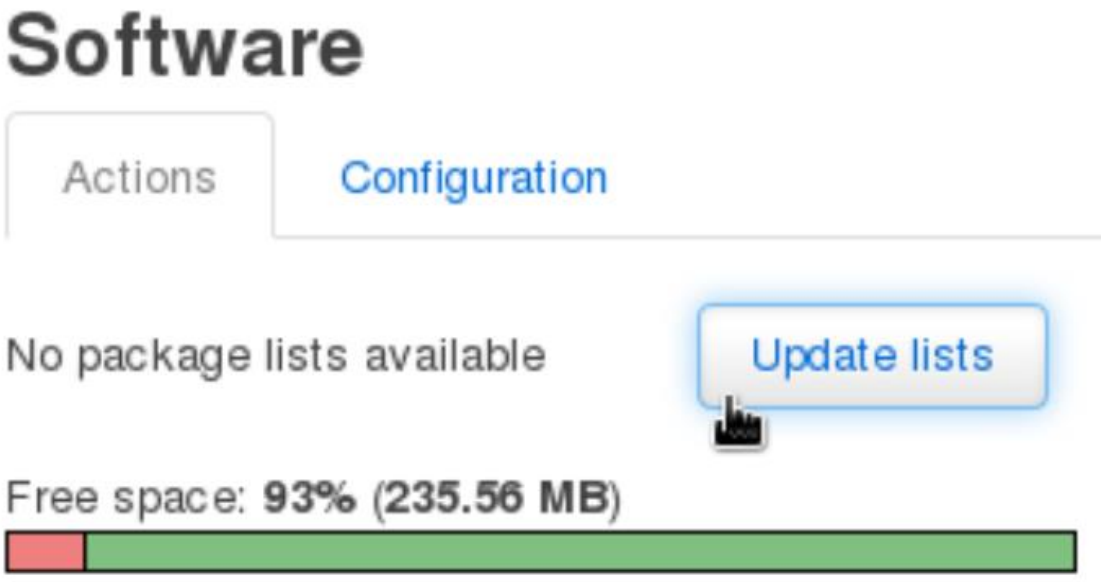
Hallintaosoitteen käyttäminen verkkoselaimessa avaa reitittimen graafisen käyttöliittymän: Käyttäjätunnus ja salasana ovat samat kuin SSH-yhteyttä muodostaessa.

ZeroTier on ladattavissa OpenWrt-käyttöjärjestelmän virallisista lähteistä. Lataaminen ja asentaminen tapahtuu System-välilehden Software-osiossa.



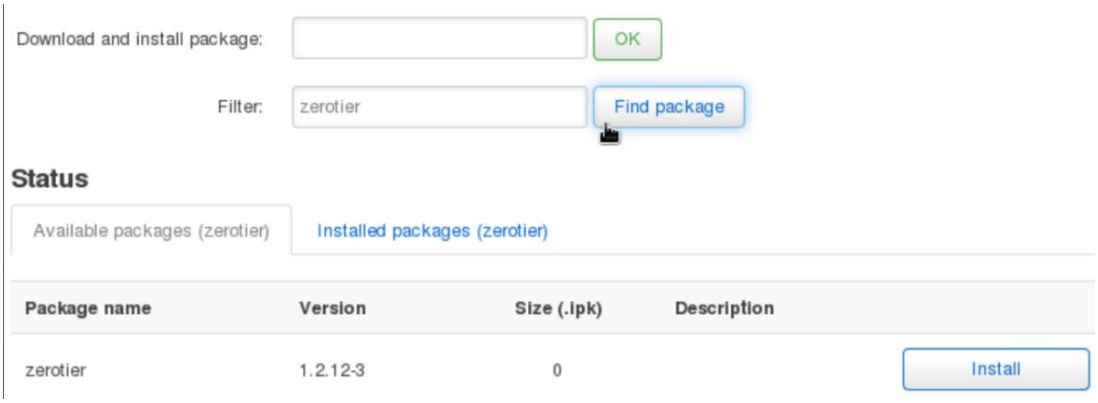
Kuva 8. OpenWrt-laitteen Software-osio

Lähteet päivitetään Update lists -painikkeella.



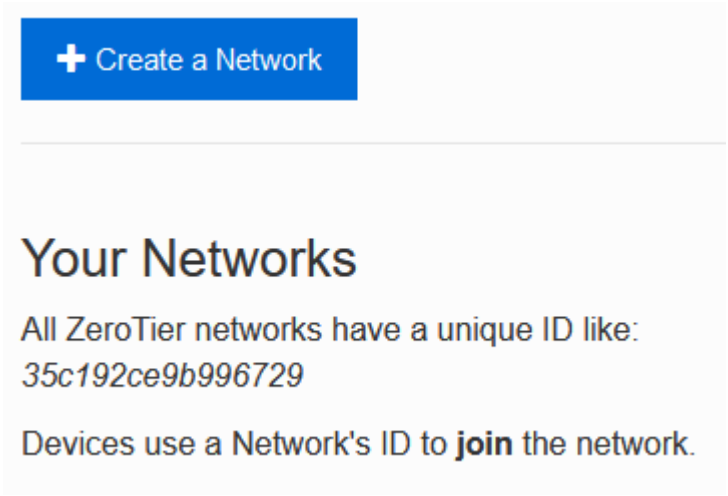
Kuva 9. Update lists -painike

ZeroTier-palvelun löytää helposti kirjoittamalla Filter-kenttään: ”ZeroTier”. Kun palvelu ilmestyy alapuolella olevaan listaan, se ladataan Install-painikkeella.



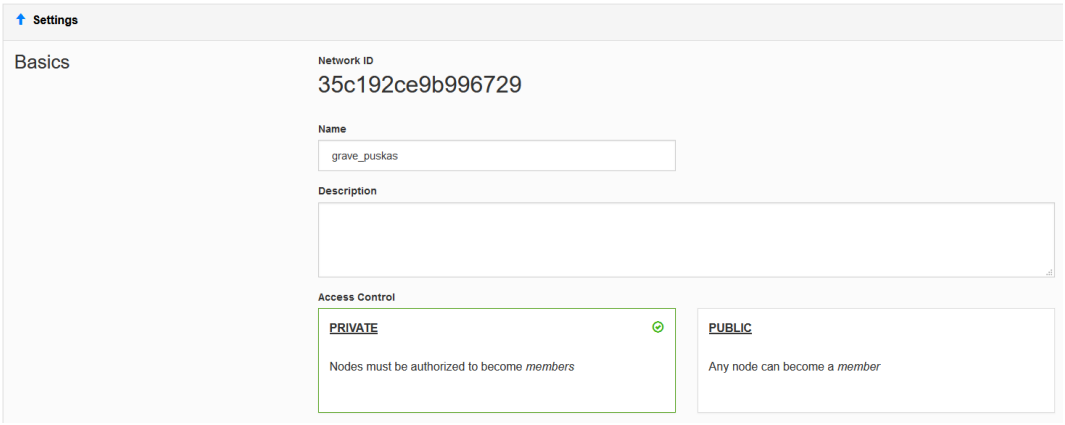
Kuva 10. ZeroTier-palvelun lataaminen

Tässä vaiheessa on hyvä luoda ZeroTier-verkko. Verkot luodaan osoitteessa https://my.zerotier.com/. Palvelun käyttäminen vaatii rekisteröitymisen. Kun kirjautuminen on suoritettu, verkkoja voidaan luoda Networks-välilehdessä Create a Network -painikkeella.



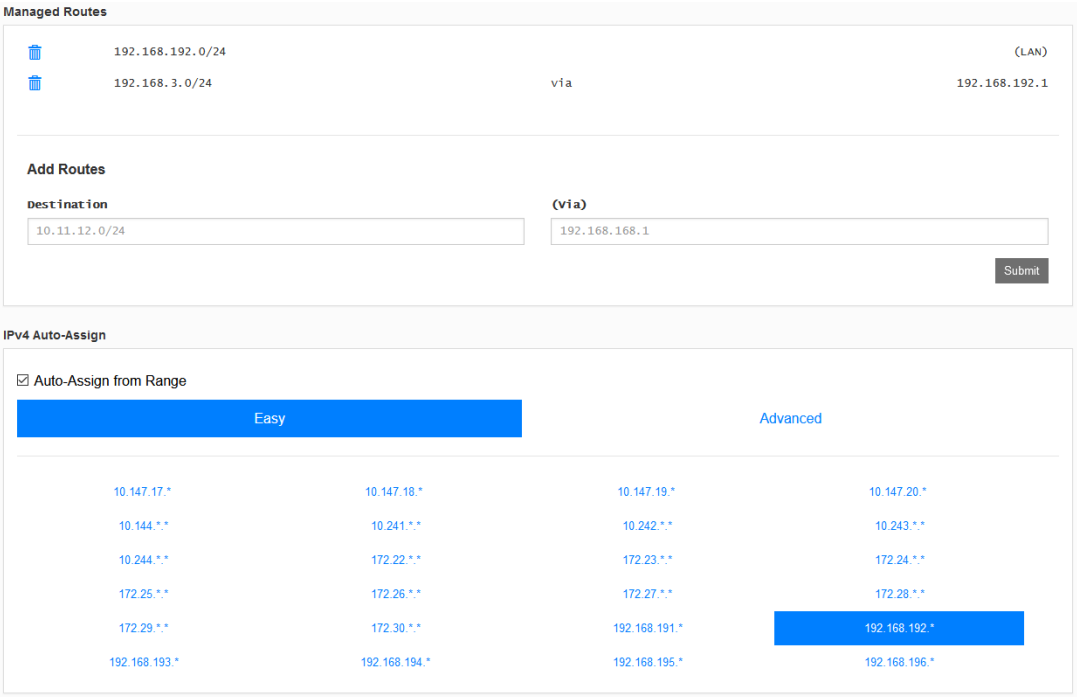
Kuva 11. ZeroTier-hallintapaneelin Create a Network -painike

Verkon tietoja tarkastellessa Settings-osion sisältä voi löytää luodun verkon ID-merkkijonon, nimen, kuvauksen ja yksityisyysasetukset.



Kuva 12. ZeroTier-hallintapaneelin Settings-osio

Advanced-osiossa verkon ylläpitäjä voi määritellä verkon reitityksiä. Tässä esimerkissä reititystauluun on lisätty sisäverkon osoiteavaruus 192.168.3.0/24, joka reititetään ZeroTier-palvelun jakamien IP-osoitteiden kautta. Tällä reitityksellä sisäverkko voidaan jakaa esimerkiksi etäkäyttäjille.



Kuva 13. ZeroTier-hallintapaneelin Advanced-osio

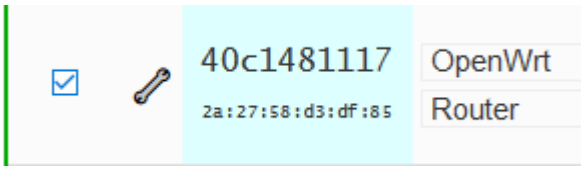
ZeroTier-palvelun konfiguroiminen OpenWrt-laitteella onnistuu tällä hetkellä ainoastaan komentokehotteella. Ensimmäiseksi reititin liitetään edellisessä vaiheessa luotuun ZeroTier-verkkoon.

 # uci set zerotier.openwrt_network=zerotier
 # uci add_list zerotier.openwrt_network.join='UNIQUE ID'
UNIQUE ID korvataan ZeroTier-verkon ID:llä, johon halutaan yhdistää.
 # uci set zerotier.openwrt_network.enabled='1'
 # uci commit zerotier
 # reboot
Reitittimen uudelleenkäynnistys on välttämätöntä.

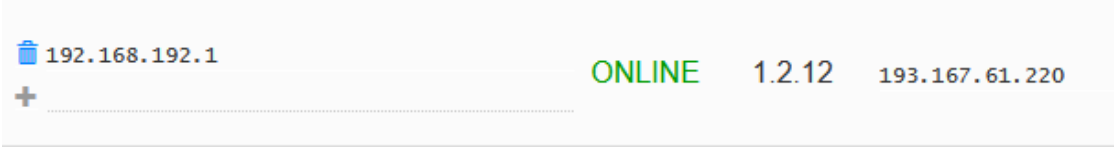
Uudelleenkäynnistyksen jälkeen OpenWrt-laitteen tulisi muodostaa yhteys ZeroTier-verkkoon. Yhteyden tilan voi tarkastaa seuraavalla komennolla:

 # zerotier-cli info

Mikäli komento palauttaa tekstin ”ONLINE”, yhteys on muodostettu.
Kun yhteys ZeroTier-palveluun on muodostettu onnistuneesti, OpenWrt-laite ilmestyy ZeroTier-hallintapaneelin Members-osioon. Mikäli ZeroTier-verkon Access Control -moodiksi on valittu Private, jokainen verkkoon liittyvä jäsen on autentikoitava manuaalisesti. Kun autentikointi on suoritettu, ZeroTier jakaa laitteelle IP-osoitteen valitusta osoiteavaruudesta. IP-osoitteen voi määrittää manuaalisesti, mikä on suositeltavaa reitittimille.

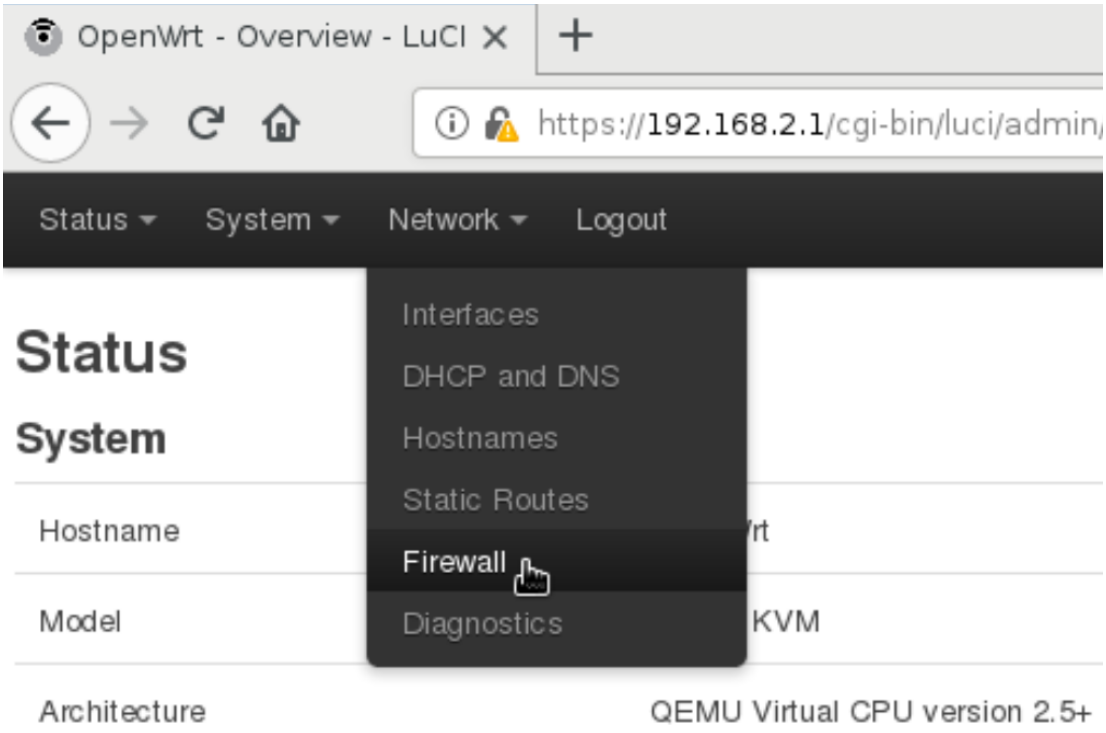


Kuva 14. OpenWrt-laite auktorisoituna



Kuva 15. OpenWrt-laitteelle asetettu kiinteä IP-osoite

Seuraavaksi OpenWrt-laitteelle asetetaan ZeroTier-palvelulle sopivat palomuurisäännöt. ZeroTier-verkot toimivat UDP-portissa 9993, joten kyseinen portti tulee avata. Toimenpide on mahdollista suorittaa graafisen käyttöliittymän Network-välilehden Firewall-osiossa.

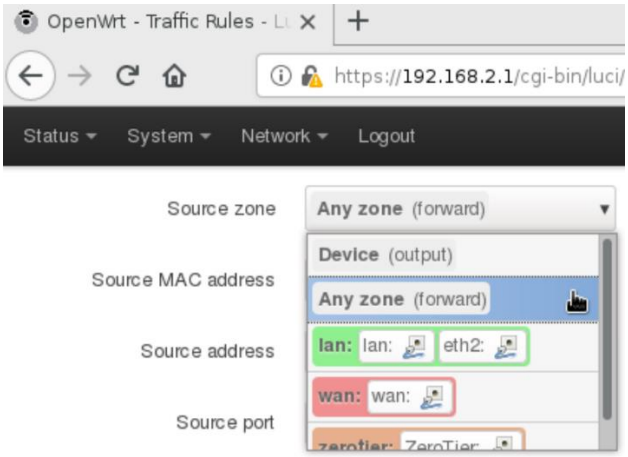


Kuva 16. OpenWrt-laitteen Firewall-osio

Firewall-osiossa valitaan Traffic Rules, johon lisätään UDP-portti 9993.

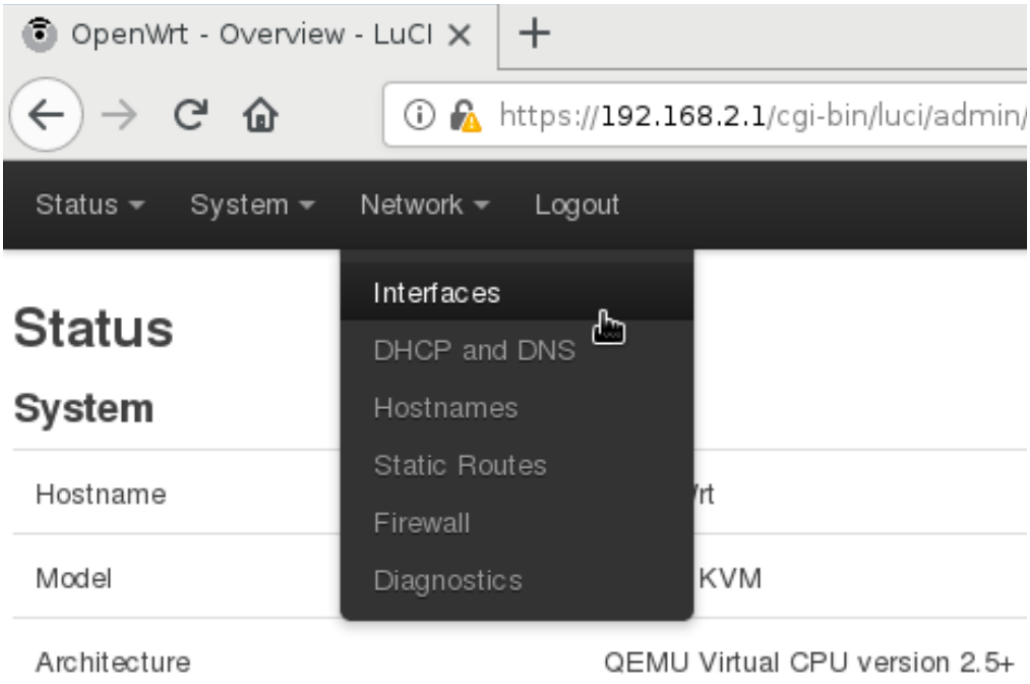
Kuva 17. UDP-portti 9993:n avaaminen

Luotu sääntö ilmestyy listan loppuun. Edit-painikkeella sääntöä voi muokata yksityiskohtaisemmin. Vaihdetaan Source zone -valinta ”Any zone (forward)”.



Kuva 18. Source zone -valinnan vaihtaminen

Sisäverkossa sijaitsevien palveluiden, eli tässä tapauksessa päätelaitteiden tulisi saada ZeroTier-verkon IP-osoite OpenWrt-reitittimen kautta. Tämä voidaan määritellä Network-välilehden Interfaces-osiossa.



Kuva 19. OpenWrt-laitteen Interfaces-osio

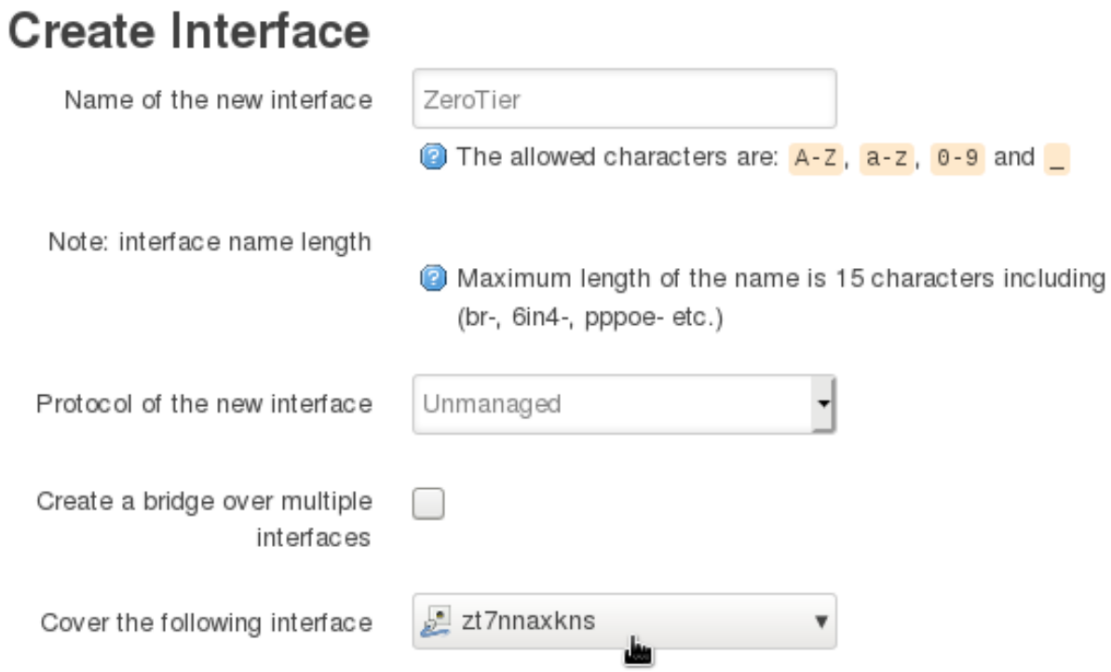
Lisätään uusi interface Add-painikkeella.

Name of the new interface: ZeroTier

Protocol of the new interface: Unmanaged

Cover the following interface: zt-merkkijono

Merkkijono muodostuu ZeroTier-verkon ID:n perusteella.



Kuva 20. ZeroTier-interfacen asetukset

OpenWrt-laitteen palomuurille on luotava uusi vyöhyke. Add-painike löytyy Network-välilehden Firewall-osiosta.

Kuva 21. Palomuurivyöhykkeen lisääminen

Palomuurivyöhykkeeseen lisätään seuraavat parametrit:

Name: zerotier

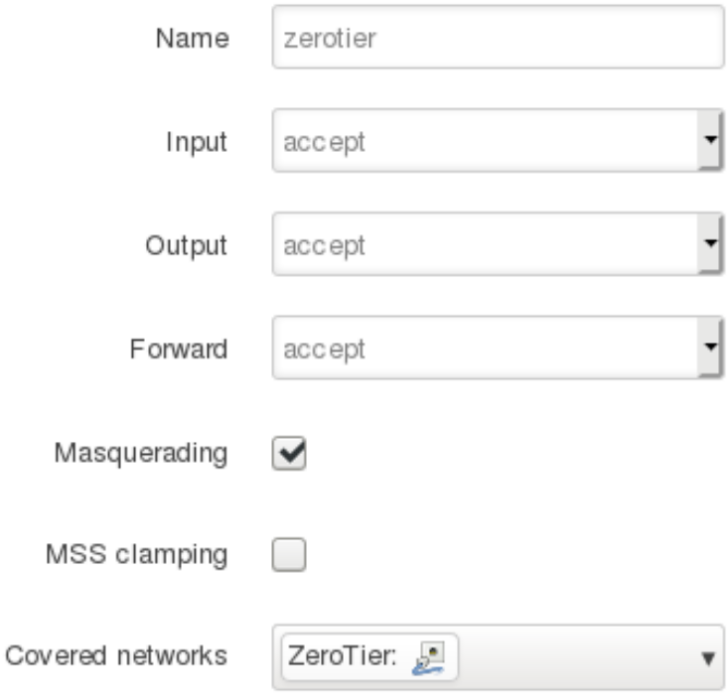
Input: accept

Output: accept

Forward: accept

Masquerading: true

Covered networks: ZeroTier



Kuva 22. Palomuurivyöhykkeen parametreja

Allow forward to destination zones: kaikki LAN- ja WAN-interfacet

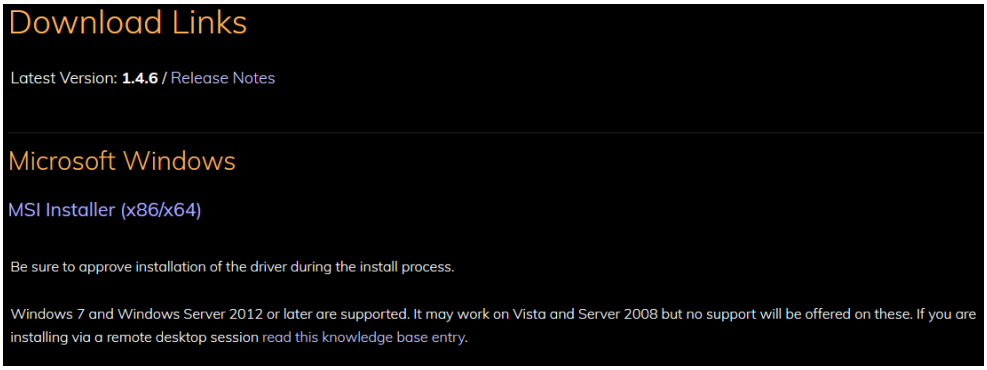
Allow forward from source zones: kaikki LAN-interfacet

Kuva 23. Palomuurivyöhykkeen parametreja

Jotta asiakaslaitteet voidaan yhdistää ZeroTier-verkkoon, niille tulee asentaa ZeroTier-ohjelmisto. Ohjelmistoa on mahdollista käyttää yleisimmissä käyttöjärjestelmissä. Tässä esimerkissä ohjelmisto asennetaan sisäverkon palveluja simuloiviin päätelaitteisiin ja etätyöntekijän sekä hyökkääjän tietokoneisiin.

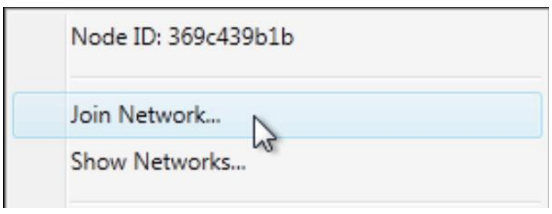
Sisäverkon päätelaitteet tulee määritellä samaan osoiteavaruuteen, joka on reititetty ZeroTier-hallintapaneelissa ohjeen aikaisemmassa vaiheessa. Tässä esimerkissä osoiteavaruus on 192.168.3.0/24. Etätyöntekijän ja hyökkääjän päätelaitteiden IP-osoitteet tulee määritellä eri osoiteavaruuteen oikeiden olosuhteiden simuloimiseksi.

ZeroTier-ohjelmiston voi ladata palvelun kotisivun https://www.zerotier.com/ Downloads-osiosta. On huomioitava, että VirtualLab-alustassa valmiina olevat Windows 7 -käyttöjärjestelmät eivät sisällä .NET Framework -kirjastoa, joka on välttämätön ZeroTier-ohjelmiston toiminnan kannalta. Kyseinen kirjasto on asennettava ennen ohjelmiston asentamista.



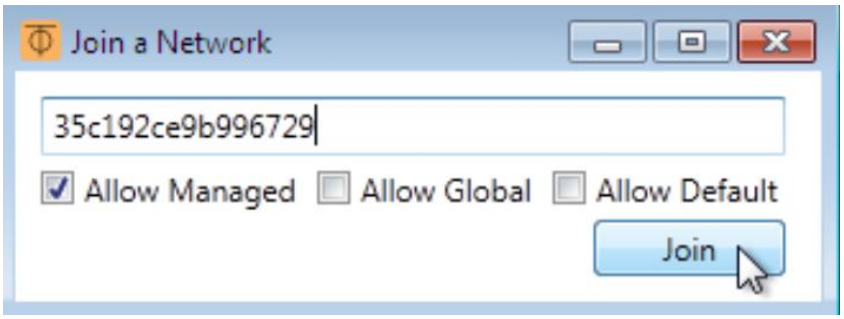
Kuva 24. ZeroTier-ohjelmiston Windows-version latauslinkki

ZeroTier-ohjelmiston Windows-versiossa ohjelmisto on käynnissä jatkuvasti tehtäväpalkin piilotettujen ohjelmistojen osiossa. päätelaite voidaan yhdistää luotuun verkkoon ZeroTier-painiketta painamalla ja valitsemalla vaihtoehdon ”Join Network…”.



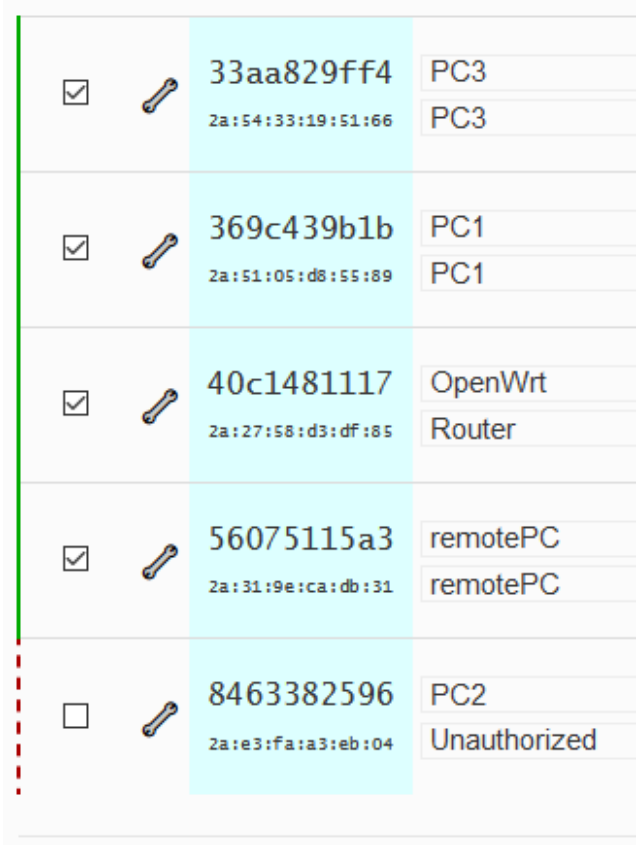
Kuva 25. ZeroTier-verkkoon liittyminen

Join a Network -ikkunan kenttään syötetään kohteena olevan ZeroTier-verkon ID-merkkijono. Merkkijonon saa selville ZeroTier-hallintapaneelista. Liittymisen jälkeen liittyvä asiakaslaite mainostaa itseään ZeroTier-palvelulle.



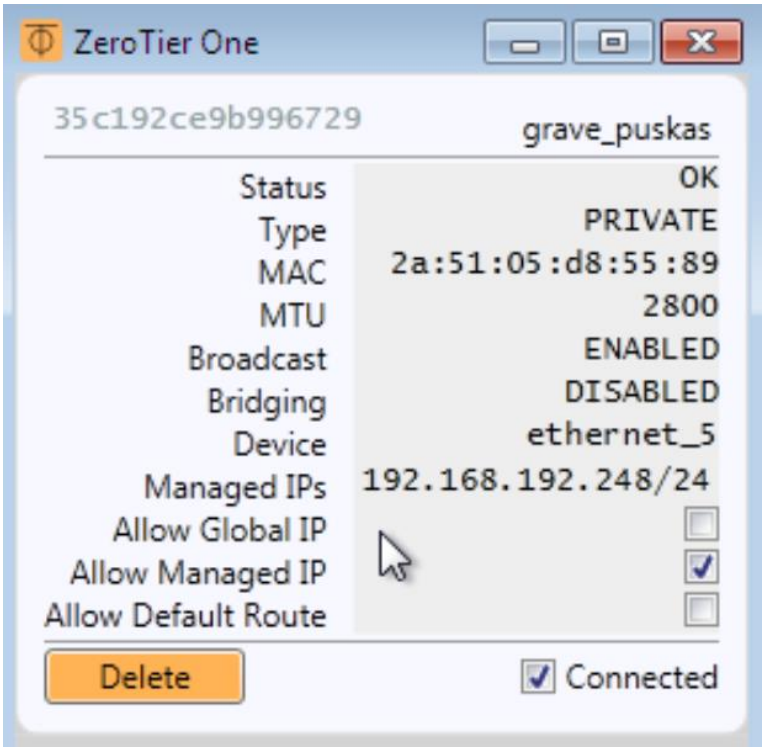
Kuva 26. Verkon ID-merkkijonon lisääminen

Liittyvät laitteet ilmestyvät ZeroTier-hallintapaneelin Members-osioon. Tässä esimerkissä ZeroTier-verkko on Private-tilassa, joten jokainen laite on autentikoitava manuaalisesti, ennen kuin ne voivat liikennöidä verkossa. Kuvassa 26 hyökkääjän tietokone ”PC2” on jätetty autentikoimatta, vaikka tämä yrittää mainostaa itseään. Laitteen identiteetti näkyy hallintapaneelissa, mutta laite ei voi tehdä mitään verkon sisällä.



Kuva 27. ZeroTier-hallintapaneelissa näkyvät verkon laitteet

Vaikka laite ”remotePC” ei kuulu esimerkin sisäverkkoon, se kykenee yhdistämään ZeroTier-verkon virtuaalisiin IP-osoitteisiin ja sitä kautta sisäverkon osoiteavaruuteen. Laite ”PC2” ei ole autentikoitu, joten sen liikenne ei pääse sisäverkkoon asti.



Kuva 28. ZeroTier-verkon autentikoitu päätelaite

Kun ZeroTier-verkko on rakennettu, hallintapaneelin Flow Rules -osiossa on mahdollista implementoida Zero Trust -arkkitehtuurin periaatteiden mukaisia tietoturvapolitiikkoja. Hienojakoiset politiikat on määriteltävä verkon tarpeiden mukaisesti, mutta yleispäteviäkin sääntöjä on. Yksi niistä on verkon liikenteen välittäminen tiettyyn ZeroTier-verkkoon valvontaa varten. Seuraavaa skriptiä käyttämällä kaikki liikenne kopioidaan laitteeseen ”33aa829ff4”, eli ”PC3”.

 # tee -1 33aa829ff4;

Kyseinen laite voisi sisältää uuden sukupolven palomuurin, joka tutkisi tällöin myös sisäverkon liikennettä. Zero Trust -arkkitehtuurin periaatteiden mukaisesti politiikoilla voidaan estää kaikki paitsi verkon toiminnan kannalta välttämätön liikenne. Mikäli haitallista liikennettä pääsisikin läpi, se kopioidaan palomuurin tutkittavaksi.

Zero Trust -verkossa käyttöoikeudet ja tietoturvapolitiikat tulisi määritellä siten, että vain välttämätön sallitaan. Alla olevaa skriptiä käyttämällä verkossa hyväksytään ainoastaan IPv4-, ARP- ja IPv6 -paketit. Tässä esimerkissä sääntö on universaali, mutta politiikat on mahdollista määritellä myös laitekohtaisesti, eli Zero Trust -arkkitehtuurille tyypillisellä hienojakoisuudella.

```
# drop
#           not ethertype ipv4
#           and not ethertype arp
#           and not ethertype ipv6
# ;
```

Tämä skripti estää IP-osoitteen väärentämisen (IP address spoofing):

```
# drop
#           not chr ipauth
# ;
```

Laitteille voidaan luoda omia ryhmiä VLAN-verkkojen kaltaisesti:

```
# tag ryhmat
#           id 1000
#           enum 100 ryhmayksi
#           enum 200 ryhmakaksi
#           enum 300 ryhmakolme
#           enum 400 ryhmanelja
#           enum 500 ryhmaviisi
```

On huomioitava, että drop-skriptejä käytettäessä Flow Rules -osion loppuun on laitettava accept-skripti, muuten kaikki liikenne estetään.

```
# accept;
```